DNSセキュリティはDNSサーバーで。SPS ThreatAvert

DNS ベースの DDoS やマルウェアに対する先進的な防御

2018年6月27日

アカマイ・テクノロジーズ合同会社　キャリア営業部　鳥巣正義

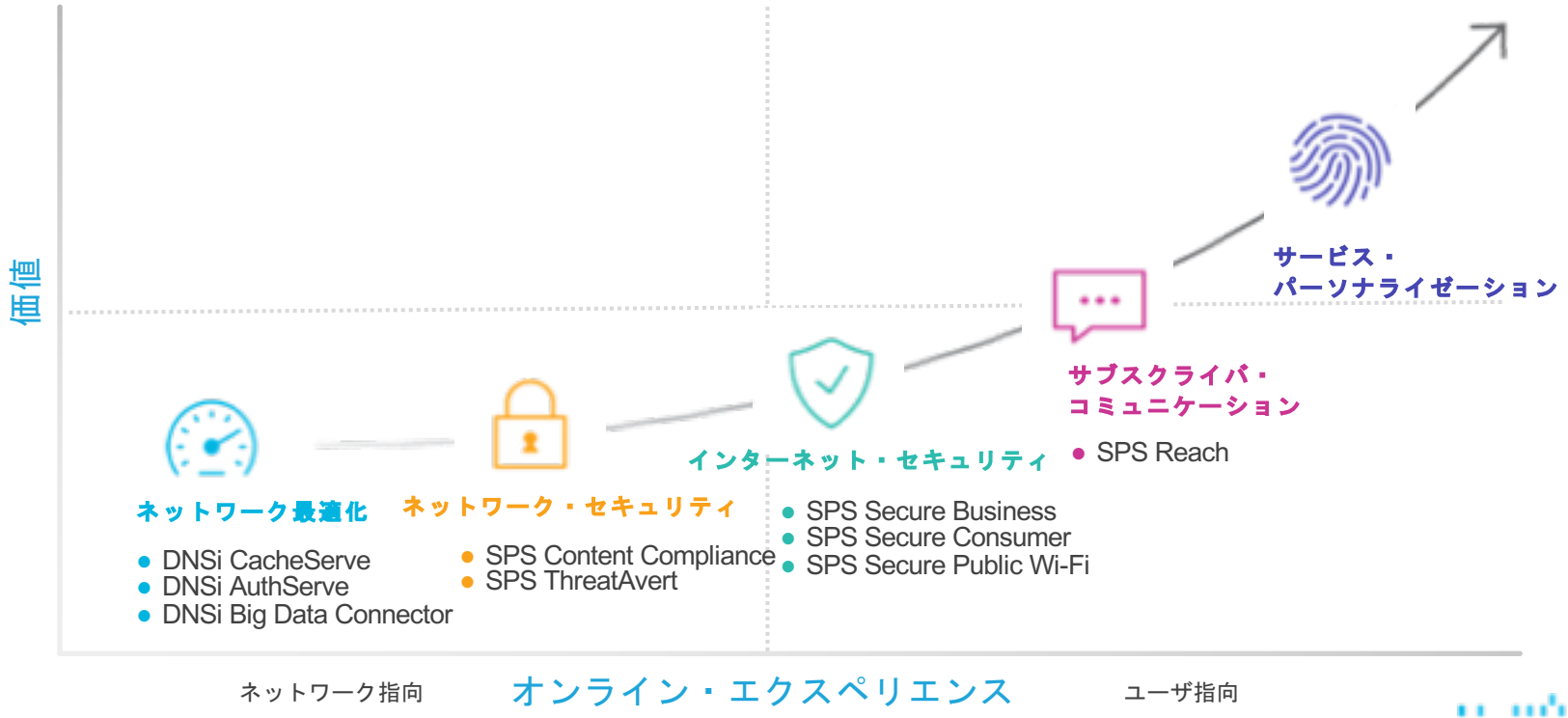
Nominum, now part of Akamai

– 今回が最後。

Akamai Technologies

- 次回から。

インターネット・サービスの向上



DNSi CacheServe – 通信事業者向けキャッシュ DNS

急なトラッフィクの増加に適用可能なスケーラビリティ

- BIND 比最大5～10 倍 の処理能力(QPS)によりサーバー数を大幅削減
- ライセンス・キーによるパフォーマンス管理による、必要に応じたスケールでの導入

エンドユーザのエクスペリエンス向上

- DNS レイテンシの大幅な減少

セキュリティと可視性

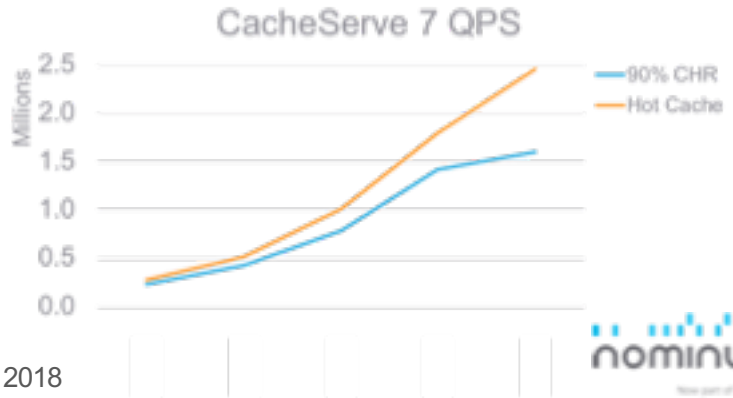
- 洗練された再帰クエリアルゴリズム
- キャッシュ・ポイズニング耐性
- 堅牢な設計による脆弱性からの解放
- パフォーマンスに影響しないクエリ・ロギングと検索
- ロードバランサやファイアウォールの排除

将来のアプリケーション

- 高精度ポリシー
- クエリ・データの収集とレポーティング

通信事業者の要求に応えるサポート提供

- ワールドワイドのサポート体制



DNS セキュリティ

セキュリティ・リサーチ: インサイトとイノベーション

50 以上の ThreatAvert の展開が2.5億以上のサブスクライバをカバー

セキュリティにおけるプレイヤー:
年 2 回のセキュリティ・レポート
データ・サイエンス・ブログ
Webinar
業界のイベントへ参加

比類ないリゾルバのフットプリント:
130 以上の通信事業者
40 ヶ国以上でのサービス
1日 1.7 兆クエリ

ビジネス及び家庭向けネットワークの保護

DNS においてネットワーク保護は重視されていなかったが..

20%

あるアンプ攻撃によって生じた解決率の低下

Source: Nominum

55%

攻撃のピーク時におけるPRSD攻撃に使われている悪意なサブドメイン

Source: Nominum

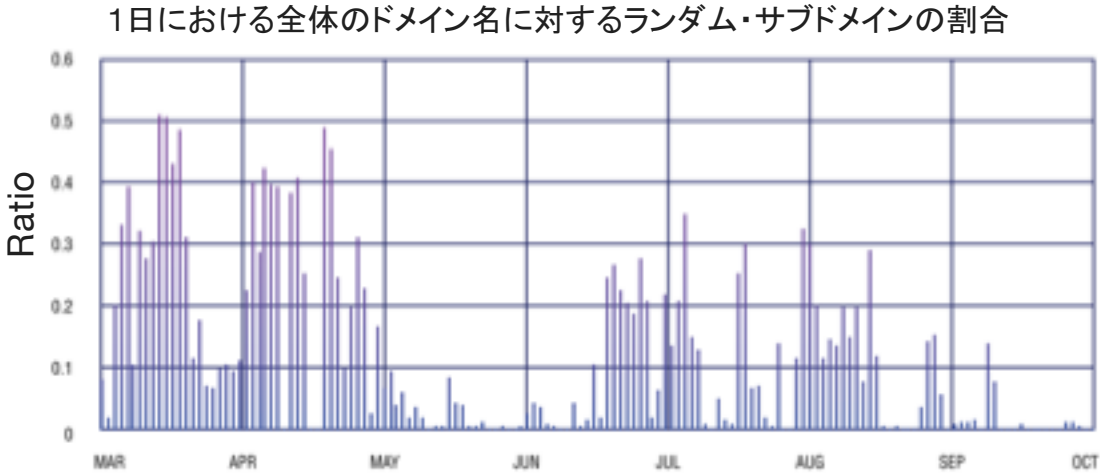
68%

2016年秋から2017年の最初の 3 ヶ月における PRSD 攻撃の増加

Source: Nominum

リゾルバに負荷を与える PRSD 攻撃の出現

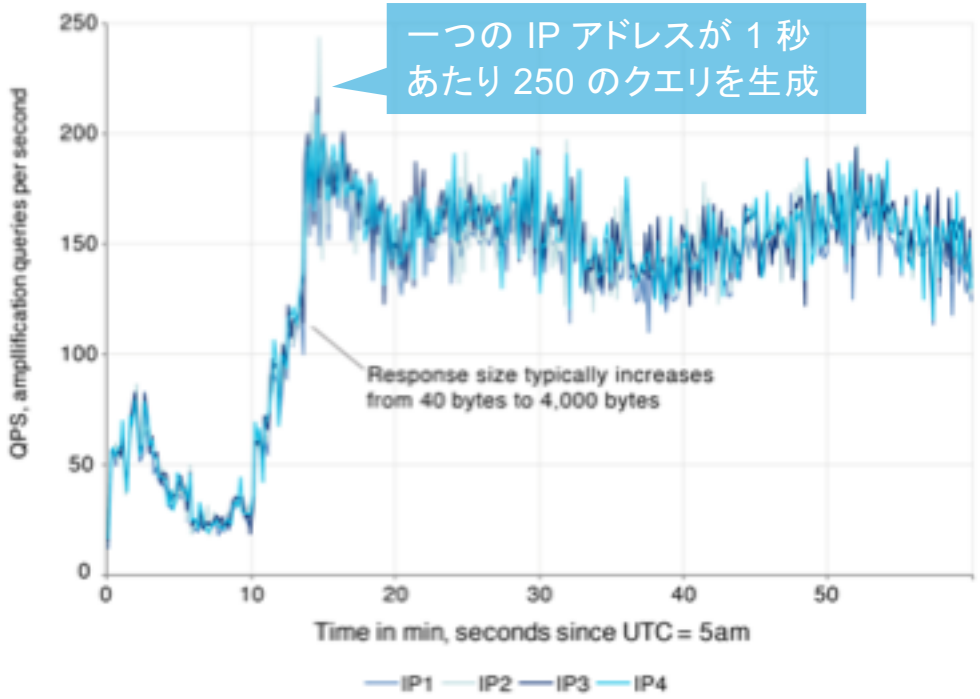
実例: 3 月の攻撃の間、全体の 50パーセント以上のサブドメインが攻撃のために生成されていた



Source: Nominum Research, 2017

アンプ攻撃は瞬時にして大きな打撃を与えうる

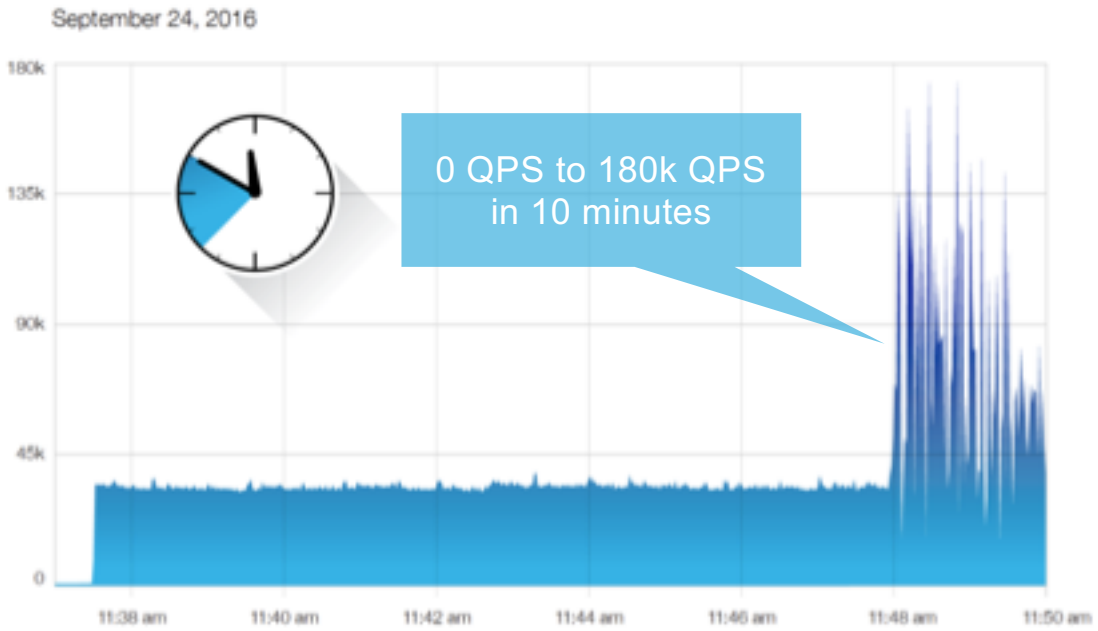
実例: 何百万ものオープン・ホーム・ゲートウェイがサーバやネットワーク・インターフェイスを飽和させうる



Source: Nominum Research, 2016 – Amplification attack traffic from 4 IPs

防御までの時間が決定的

実例: 数分のうちに QPS は上昇し、被害を生じさせる



Source: Nominum Data Science

新しい攻撃の迅速な検出

予測済み

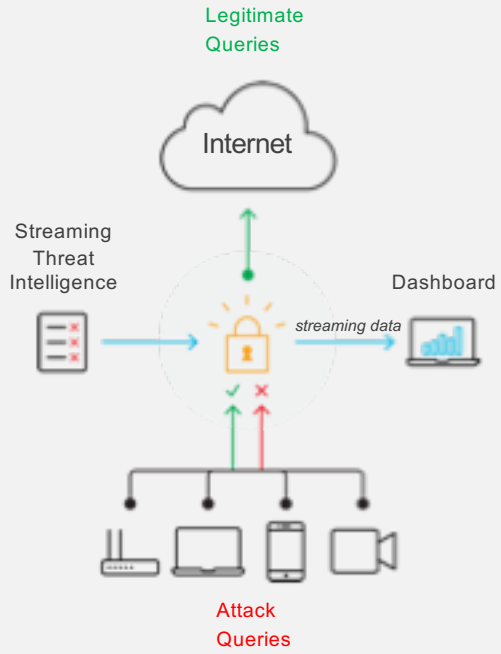
DDoS

その他の脅威

nominum

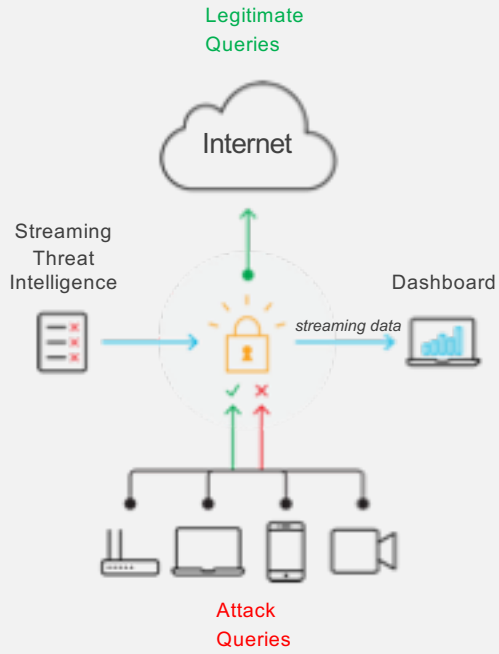
ThreatAvert による防御のしくみ

SPS ThreatAvert



- Akamai からフィードされたリスト、CacheServe でネットワーク・セキュリティ・ポリシーを適用
  - ボットネット C&C（コマンド・アンド・コントロール）のブロック
  - DNSアンプ攻撃に対するブロックやレートリミットによる抑制
  - ランダム・サブドメイン攻撃（PRSD / 水責め）のブロック、抑制
  - DNSトンネリングのブロック
- レポート
  - 検出・ブロック状況
  - ドリルダウンによる詳細（脅威別、マルウェア・タイプ、クライアント毎など）
  - 定期的なレポート作成
  - エグゼクティブ・レポート

DDoS、ボット、マルウェアの抑止



先進的なリサーチによる後ろ盾

ノミナム・セキュリティー・リサーチ は独自の手法と機械学習により 1 日あたり 1000 億以上のクエリを解析している。

専用に作られたシステムは

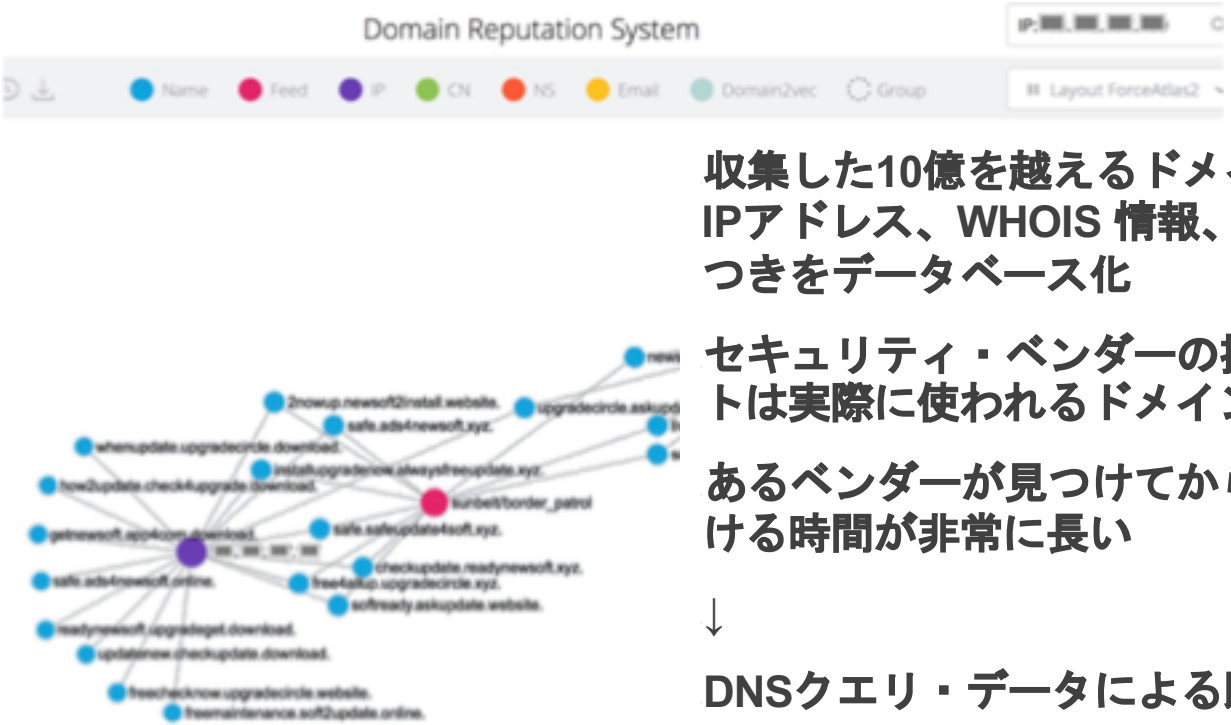
- 秒速で特異性 (anomaly) を検出
- 継続的にドメイン・レピュテーションを計算し、新たに出現した脅威を特定
- 機械学習を用いてカバー率を拡大
- 偽陽性 (false positive) を排除するための相関関係チェック

事前防御

脅威情報のアップデートは継続的に配信され即時にブロック

- DDoS 攻撃によるネットワークへの被害を瞬時に開始、停止
- ボットがネットワークやデバイスに影響を与えることによるサブスクライバのエクスペリエンスの低下を抑止

ドメイン・レピュテーション・システム (DRS)



収集した10億を越えるドメイン名と、NS、CNAME、IPアドレス、WHOIS 情報、各種リスト、などの結びつきをデータベース化

セキュリティ・ベンダーの提供するドメイン名のリストは実際に使われるドメイン名の一部にすぎない

あるベンダーが見つけてから次の別のベンダーが見つける時間が非常に長い

↓

DNSクエリ・データによる既存のリストの拡張が有効

nominum

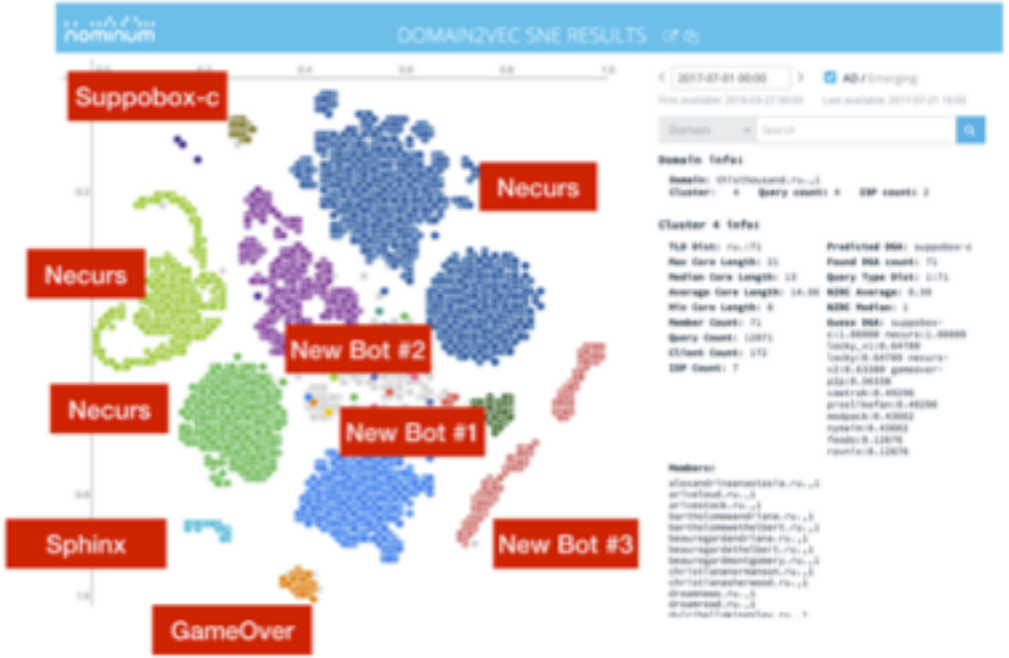
Domain2Vec

ドメイン名間のクラスタリングにより、既存のリストでカバーされていないドメイン名やDGAの発見

- 文字列のパターン
  （TLD、長さ、文字種…）
- 解決した IP アドレス
- クライアント IP アドレス
  （数、頻度、ネットワーク…）
- 権威 DNS
- 登録者
- 前後にクエリされているドメイン名

:

90以上の属性によるクラスタ解析を自動的、継続的に実施



高精度ポリシー：正当なトラフィックを保護し悪質なトラフィックをブロック

サブドメイン・ブロック

PRSD の一部はポピュラーなドメインを狙う
CacheServe のポリシーは、正当なサブドメインを許可し、その他のサブドメインをブロック

レート・リミット

アンプ攻撃の中にはANYクエリが用いられるものがある
CacheServe のポリシーで ANY クエリにレート・リミットを適用

truncate

レート・リミットにおいて閾値を超えたクエリには truncate 応答を返す
正当なクライアントならば TCP でリトライ
スプーフ(詐称)されたアドレスへの truncate 応答はリトライされない

$*? $*?

ThreatAvert のレポーティング

データ・アーキテクチャ

実績あるスケーラビリティと処理能力

- 世界中の大規模ネットワークで実証されたオープンなコンポーネント

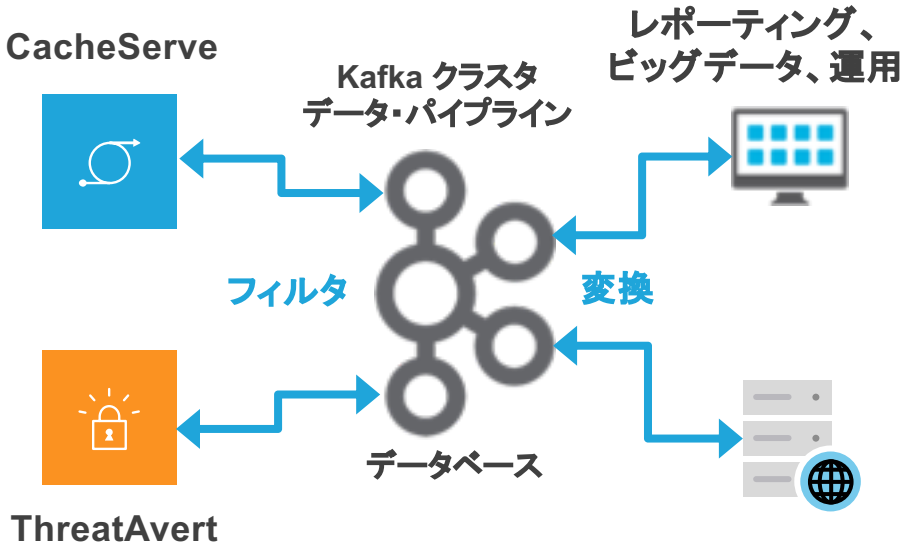
無停止の可用性

- 堅牢なアーキテクチャによってダウンタイムを抑制し、アップグレードも行いやすく

広範囲に活かせるリアルタイムの DNS データやテレメトリ・データ

- ビッグデータ・システム (Splunk、Hadoop 等) や他のアプリケーションへの高信頼の接続性

リアルタイムの DNS データを必要とされるところにエクスポート:

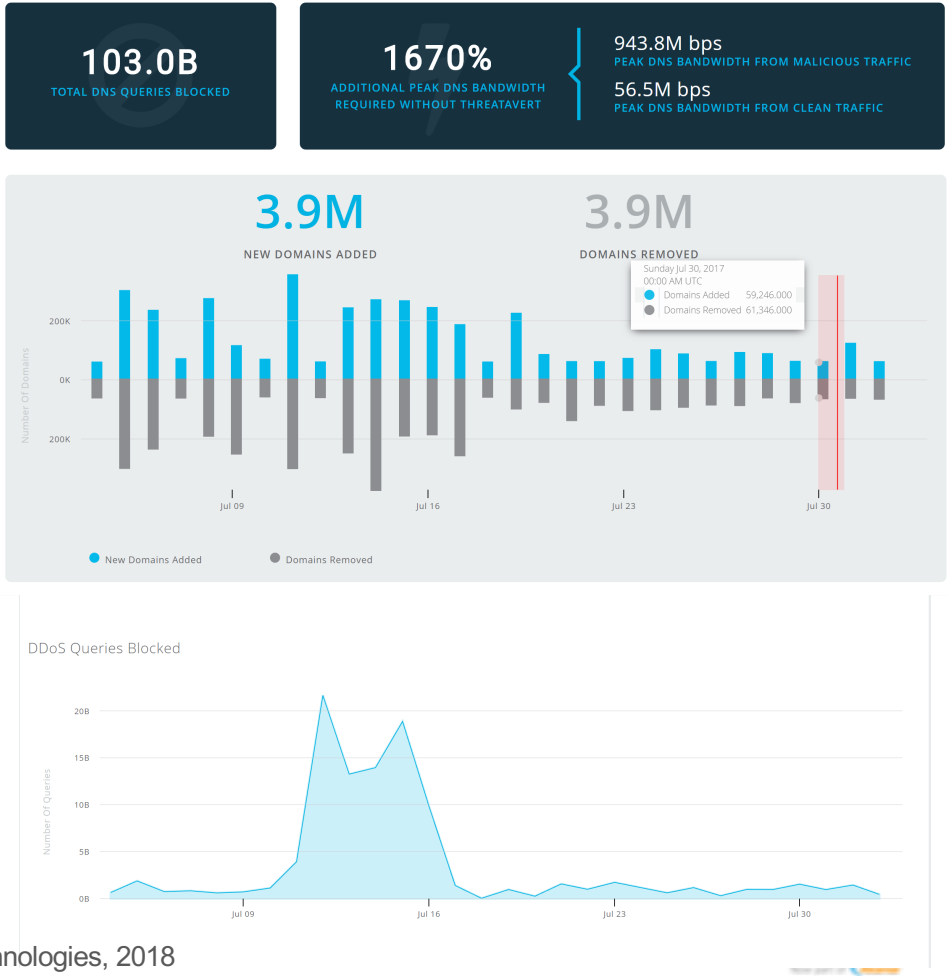


- アプリケーション・ポータル
- 既存のビッグデータ・システム
- その他の運用システム

エグゼクティブ・ダッシュボードによる脅威の俯瞰

- ブロックされた DNS クエリ – 抑制された悪質な活動を表す
- 節約できたピーク DNS 帯域 – 節約できたコスト
- リスト・アップデート –リスト更新状況の可視化
- 感染サブスクライバ数 – ネットワークへの攻撃の窓口であり、影響を受けている顧客でもある
- ネットワーク内のマルウェア – 脅威の一覧

レポーティングは ThreatAvert のベースに含まれており追加のライセンス不要



脅威の詳細を表示するセキュリティ・ダッシュボード

- カテゴリごとのグラフ
  - DNS アンプとランダム・サブドメイン攻撃 (PRSD) - QPS とトップ 10 ドメイン
  - マルウェアのクエリ数と感染した IP アドレス数
- ワン・クリックで詳細のレポート
- DDoS の経時レポート (5分単位)
- 個別の DDoS やマルウェア・ドメイン、クライアントの詳細

運用に求められるインサイトをワン・ストップで提供

オペレーション・ダッシュボード - DNS クエリへの洞察

- QPS、クエリ・タイプ、レスポンス・コード
- リカージョン・コンテキスト
- リクエストとレスポンスの帯域

システム・レポート - 運用におけるキーとなる情報を表示

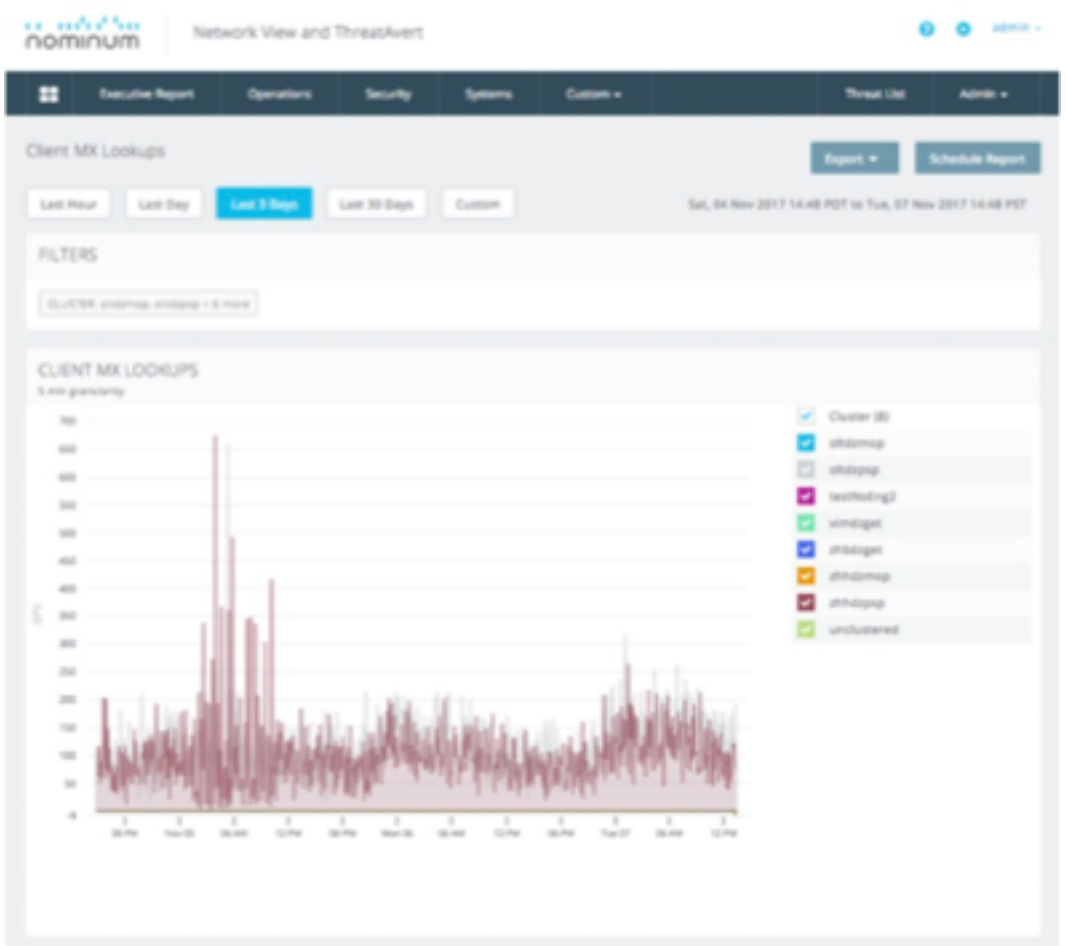
- クライアント＆権威リクエスト / レスポンス
- キャッシュ・ヒット / ミス
- UPD/TCP リクエスト
- スレッド毎のCPU使用率、メモリの使用率

カスタム・
ダッシュボードと
カスタム・レポート

任意のデータセット

必要に応じてグラフや表で表示

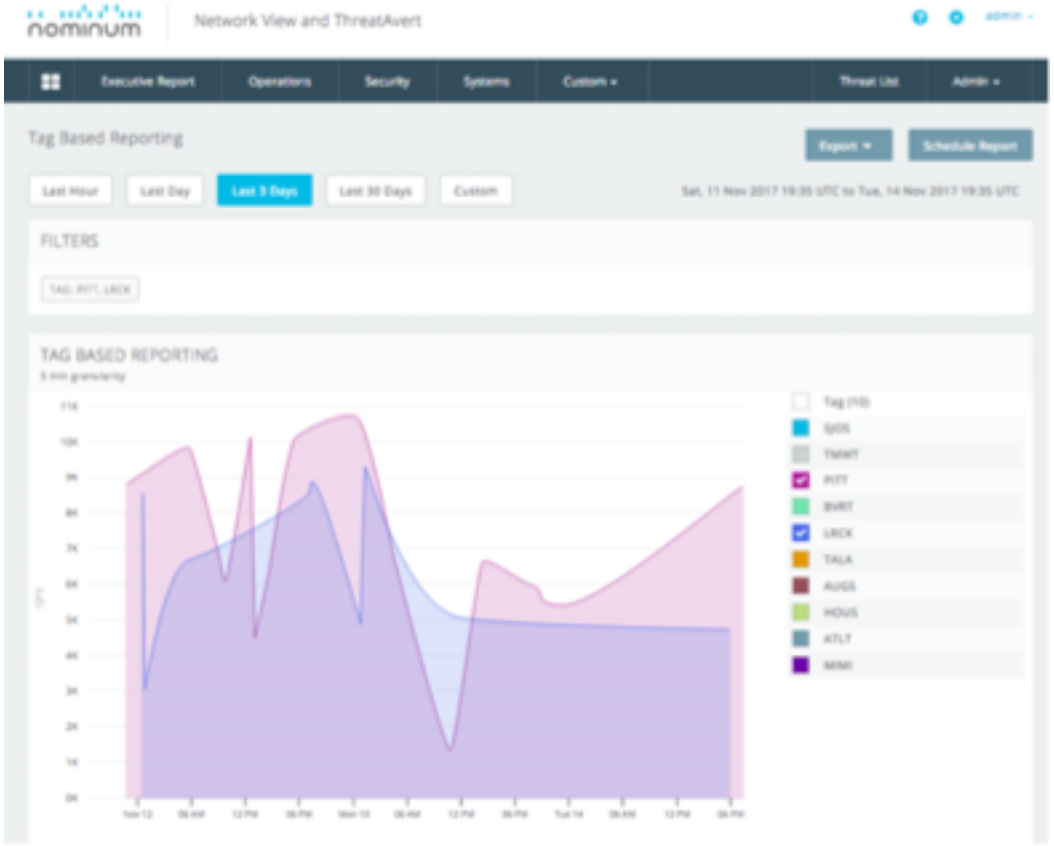
スクリプト処理や、外部での加工を不要に



ネットワーク・トポロジーやその他の運用上の要求に応えるレポート

セグメント毎のレポート

- 固定系と移動体、 都市や地域、IPv4とIPv6など.
- ユーザの定義したサーバ・グループをタグとしてレポート



ヨーロッパにおける激しい DDoS 攻撃の抑止

課題

- 毎日異なるドメインをターゲットとした DNS クエリがネットワーク・トラフィックの 70% に影響

ソリューション

- すでに CacheServe が使われていたため、迅速に ThreatAvert を有効化
- 攻撃を解析してフィルタを設定したりといったマニュアル・オペレーションが不要に

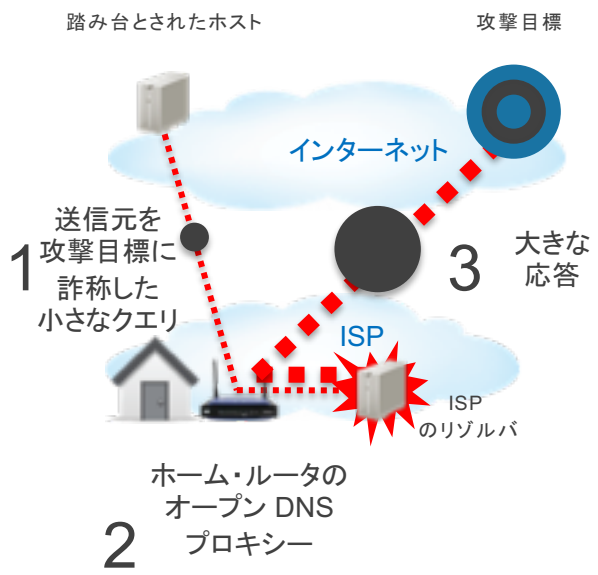
結果

- 悪質なクエリが識別され、サービスが正常に戻った
- 1年あたり €200,000 の継続コスト削減
- 1件あたり €50,000 かかったサポート・コスト削減

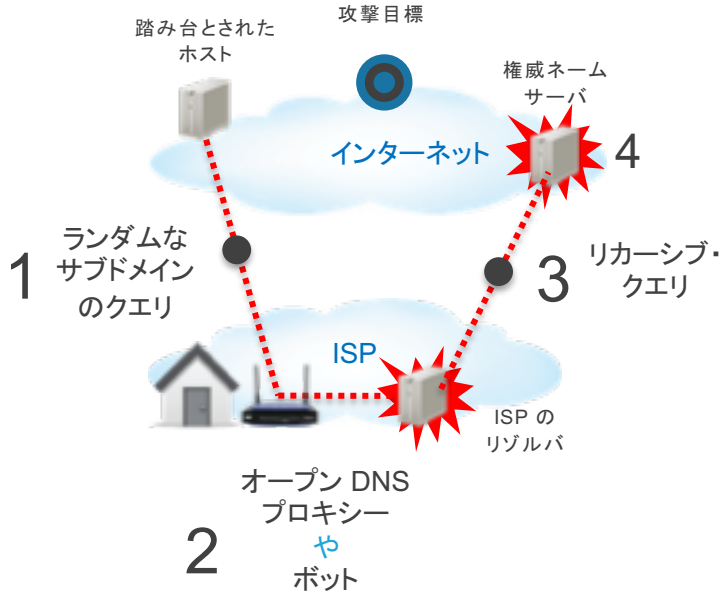
追記

攻撃のしくみ

アンプ攻撃



ランダム・サブドメイン攻撃



データ・インテリジェンスへの貢献

DNS データをビッグ・データ・システムに投入
サブスクライバに対するデータを集成。
追加のハードウェアは不要

シームレスな統合
Hadoop や Splunk への取り込みが可能で、すぐに解析に加えることが可能

スケーラビリティ
シンプルなデプロイメント、転送時 80 %のデータ圧縮