DNS データ・サイエンス
Internet Week, Tokyo Japan

Bruce Van Nice
Nominum

Nominum について

- Paul Mockapetris
- BIND 9 を設計したエンジニア
- 40カ国以上で使用
- 日々4億加入者以上が使用
- 日々1.8兆のトランザクションを処理

自己紹介

- Nominumのプロダクト・マーケティング・ディレクター
- DNSセキュリティを中心
- 業界のイベントに積極的に参加
- ネットワーク業界歴30年以上

なぜDNSデータの調査をするのか?

- 既存の脅威分析が不充分
  - DNS DDoSがカバーされない
  - ボットやマルウェアが充分にカバーされない
- 既存のフィードの限界:
  - 受け入れられない水準の偽陽性
  - 通信事業者としては使えない
- 複数組み合わせたからといってよくはならない。

BAD + BAD ≠ GOOD !

DNS データ・サイエンス

パターンと関係の発見

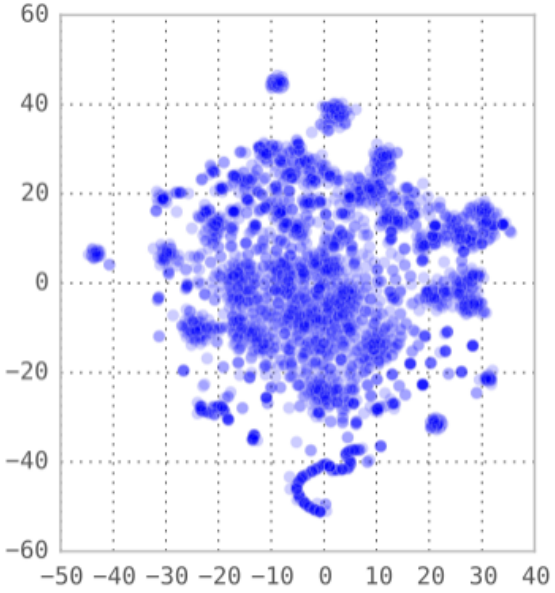
- 3.5 テラバイト/日以上のデータ
- 3%近くのISP DNSトラフィック

データはプライバシー保護のため匿名化処理

関連付けの技術

- 機械学習 – 類似性を探索
  - sfgiants.com google.com redsox.com mlb.com facebook.com…
  - botnet_cnc1.com google.com botnet_cnc2.biz facebook.com yahoo.com botnet_cnc3.ru

- お互い似通ったドメインのグループを視覚化



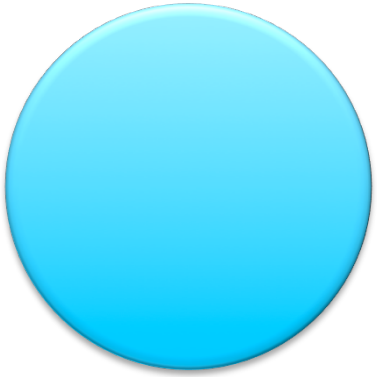
関連付けの技術によりマルウェアの発見がより速く

他の関係を顕在化 – 同じマルウェアに感染した別々のアプリ

例: 新しいコア・ドメイン

DNSデータから:
ほぼリアルタイムで
1日350万

多くがDGA(アルゴリズム生成)
多くが有害
解決できないものも多い



List 1:
9,800

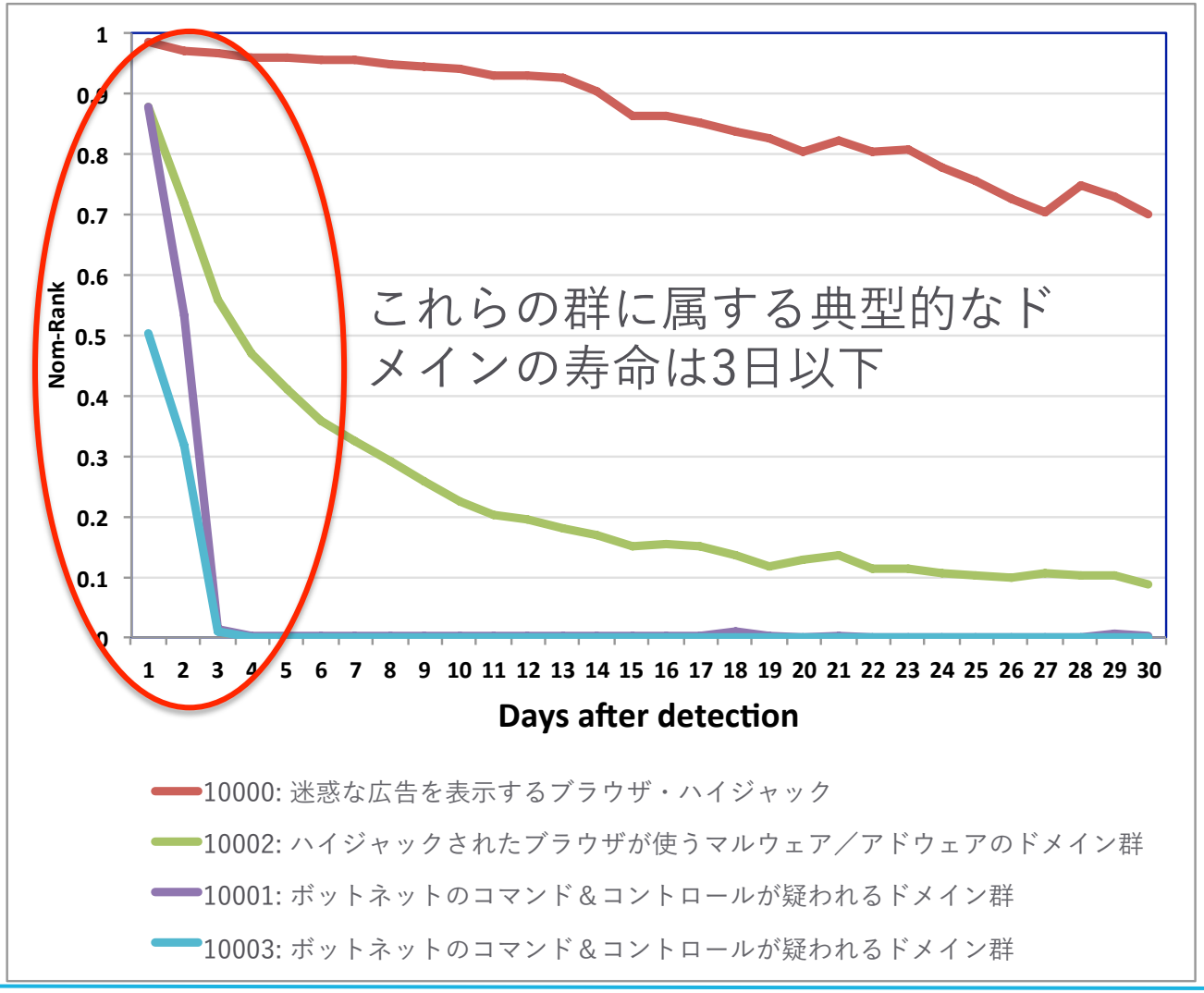
List 2:
9,100

List 3:
6,000

他のリストで27日
経ってレポート

nominum

例：検出された群


これらの群に属する典型的なドメインの寿命は3日以下
Nom-Rank
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
Days after detection
10000: 迷惑な広告を表示するブラウザ・ハイジャック
10002: ハイジャックされたブラウザが使うマルウェア／アドウェアのドメイン群
10001: ボットネットのコマンド＆コントロールが疑われるドメイン群
10003: ボットネットのコマンド＆コントロールが疑われるドメイン群

例：ブラウザ・ハイジャック

- ネットワークにより1%から20%の感染率のマルウェア・パターン
- ブラウザ・ハイジャックと不明な有害動作
- 1日に複数回のコマンド＆コントロール(CNC)のクエリをし続ける
- アルゴリズムにより感染したPCを判別
  - CNCトラフィックはブロック・またはモニタ
- 停止して何日も経って脅威リストに載ってくる

ドメインの例

acapulcosonars.com.
enticingsuperpower.com.
envelopspunnet.com.
evocationsmotliest.com.
heronsquadrupled.com.
infernalbrazing.com.
joininguncoils.com.
mumbleinterim.com.
pancakeskennels.com.
pesterlipid.com.

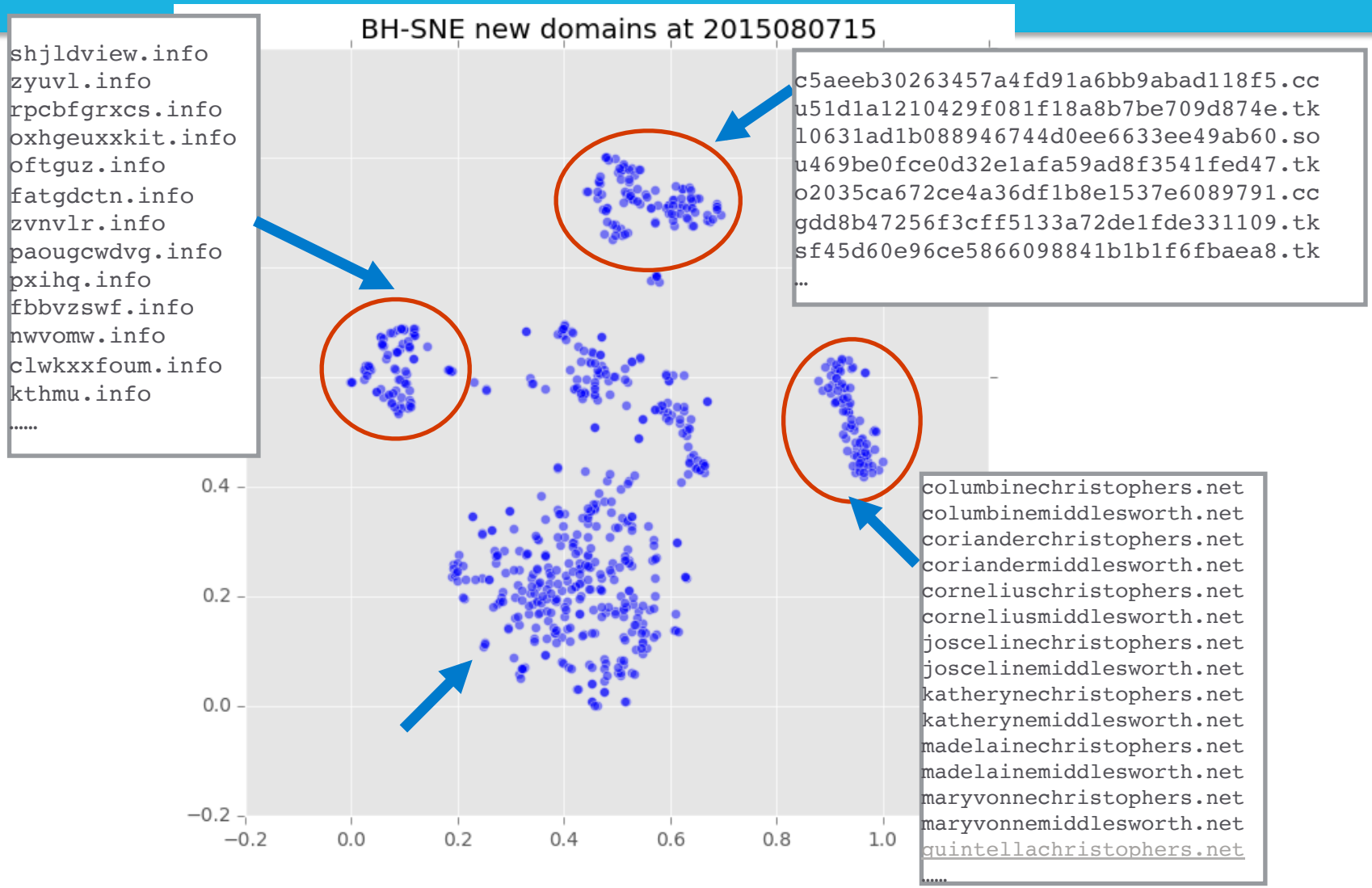
例：アド・トラッカー

- Webサイトでは多くのアド・トラッカーが使われる
- 知られたアド・トラッカーをシードとし
- クエリ・パターンの関連を探索

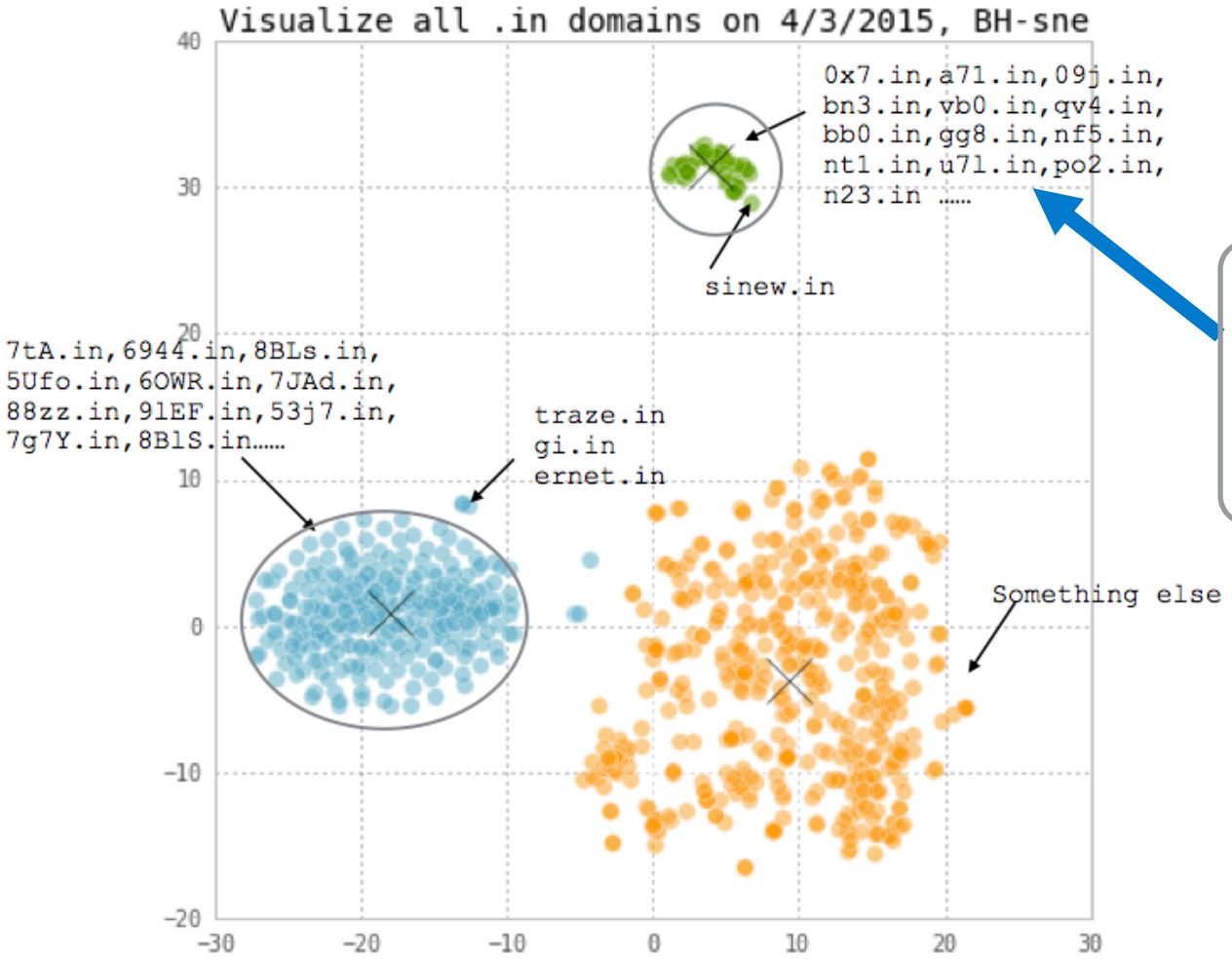
ドメインの例

2082.info.
6485.info.
7228.info.
daap.info.
drab.info.
fiiy.info.
flob.info.

例：ボットネット・クラスタ



例：DNSトンネリング



トンネリング検出アルゴリズムで再検査、確認

まとめ

- DNS データは多くの興味深いことをあらわに
- DDoS
- ボット/マルウェア
- アドウェア
- トンネル

- 他にももっと多くの発見があるでしょう

Thank You!