MWS・CSS2010 発表用資料

プリズムマップによる可視化を用いたマルウェアの動向解析

Little eArth Corporation

2010/10/19

株式会社ラック
サイバーリスク総合研究所
マルウェア解析研究所

金子　博一

目次

- 背景
- 目的
- 情報可視化
- 可視化システムの説明
- デモ
- 可視化結果
- まとめ

背景

- コンピュータを狙ったサイバー犯罪の発展
  - ゼロデイ攻撃　(2010年7月～9月に規定外緊急パッチの適応)
  - Stuxnet
- 対解析・セキュリティを考慮したマルウェアの登場
  - ゼロデイを利用したマルウェア
  - 亜種
  - 難読化

日々セキュリティベンダーはこれらの脅威に対抗している
⇒攻撃の特徴を掴むことは対策を打つ為に重要

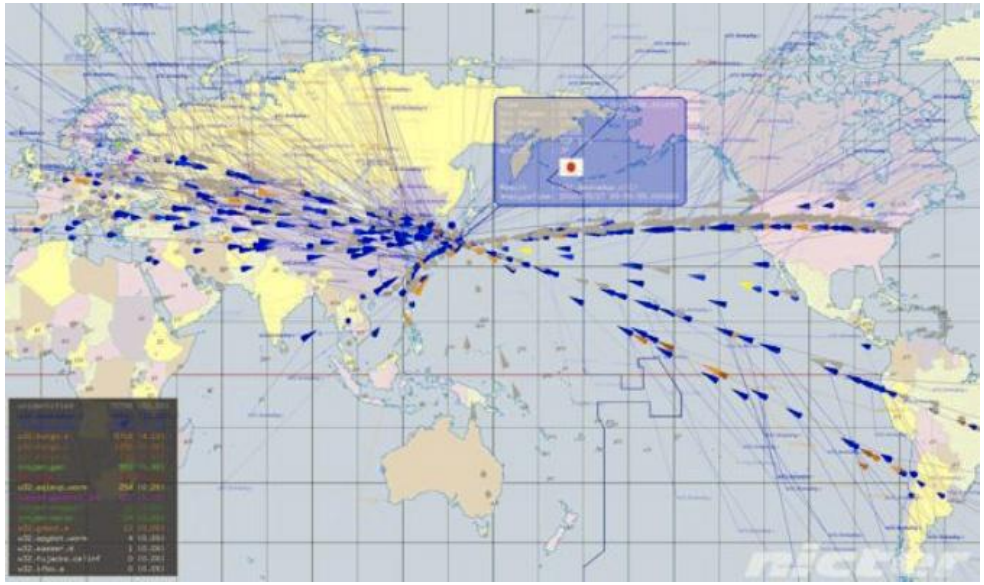
目的

- 検体の特徴把握
  - 悪用する脆弱性と傾向
  - 攻撃者の意図と選択されやすい検体・攻撃

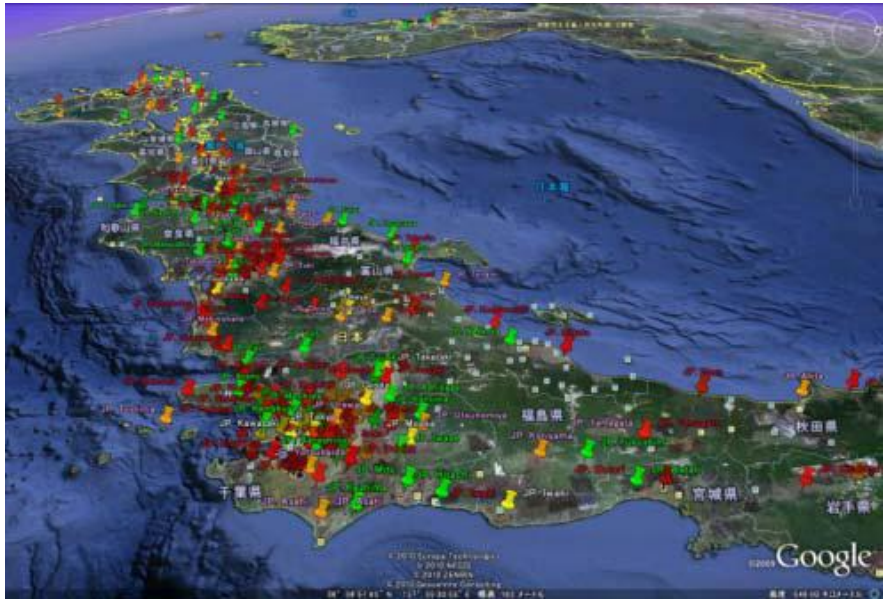
- 攻撃状況理解の促進
  - 人にわかりやすい表現手法
    - わかりづらいものをわかりやすくする
    - 詳細な解析の取っ掛かりを掴む
  - 必要に応じて詳細な情報を出す
    - インタラクティブ性
    - ユーザの入力による動的操作

情報可視化

- 人に情報を伝える手法の一つ
  - 多すぎる/理解しづらい情報を効率的に人に伝える
  - 人と親和性が高く直観的に理解しやすい

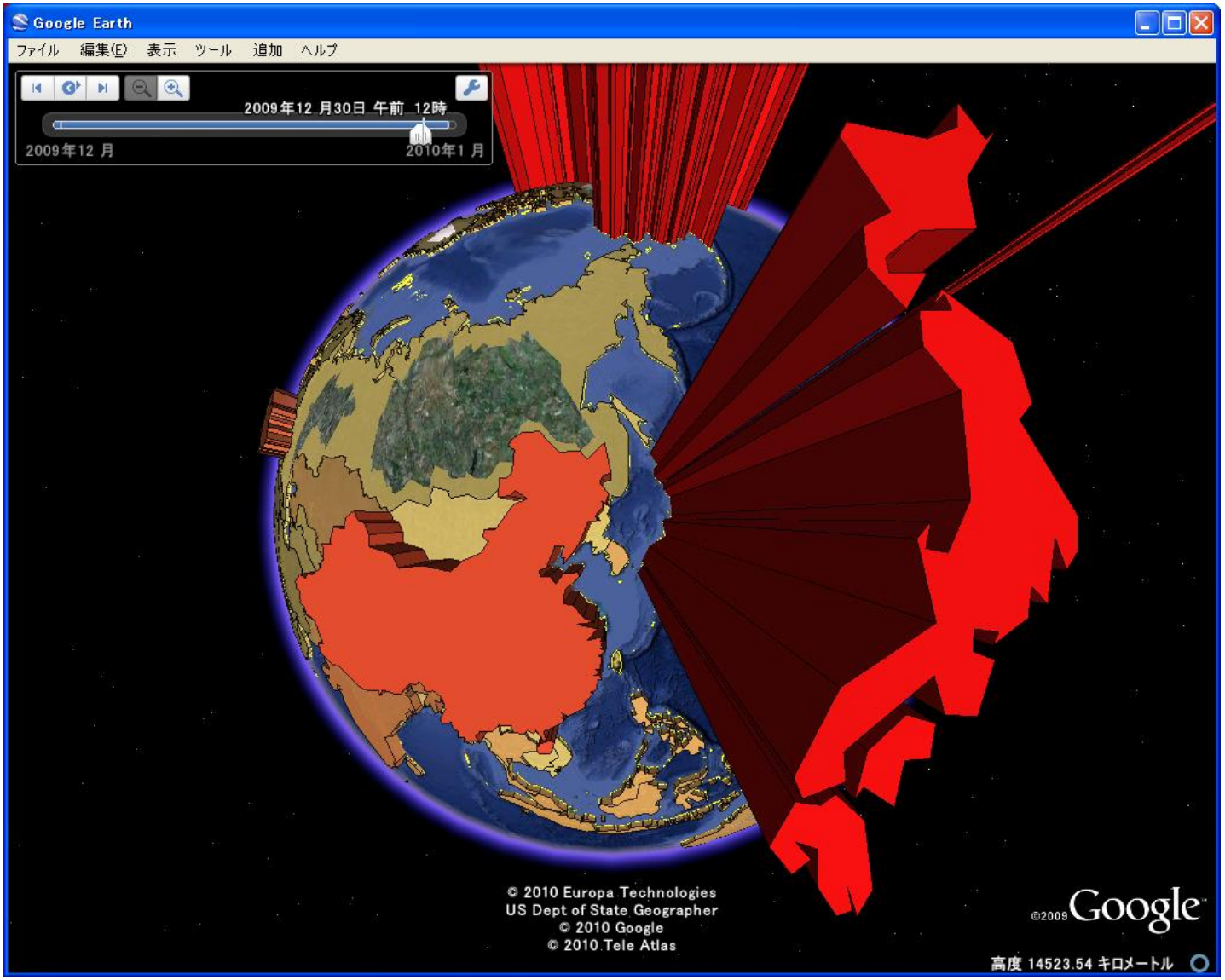


nicter



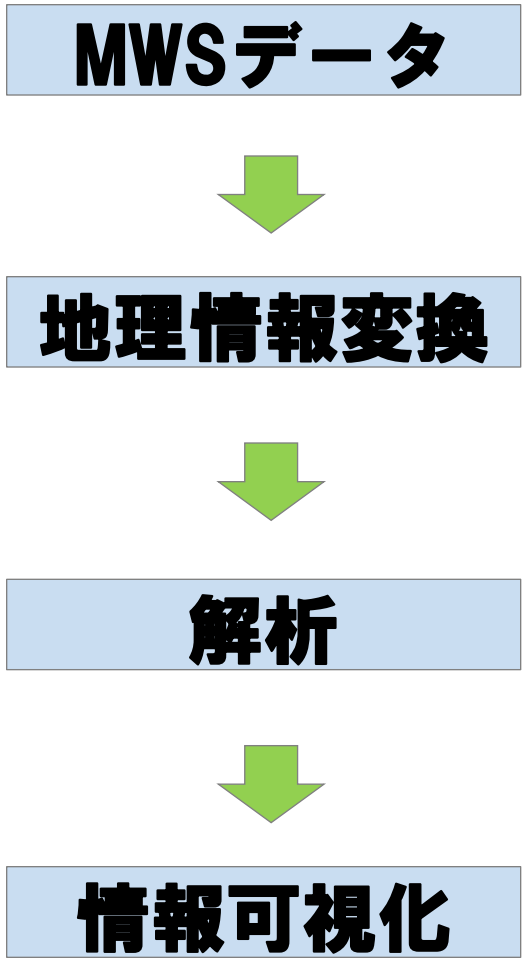
Winnyスーパーノードの可視化

可視化システムの説明 – 外観



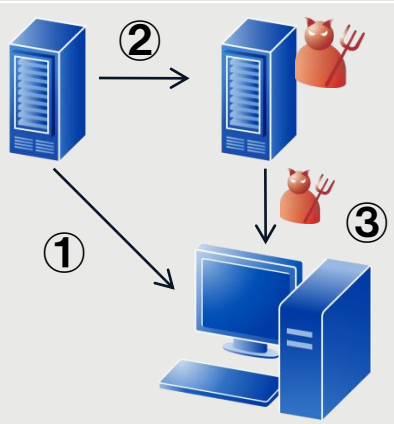
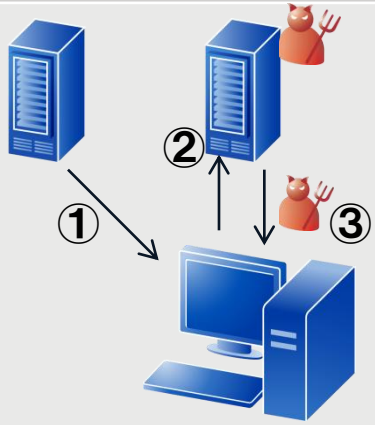
可視化システムの説明 – 概要

- **MWSデータ**
  - 扱うデータの時間は適量を目指す
  - 可能な限り多くの項目を扱う
- **地理情報変換**
  - 最小単位の設定(大陸、国、州/県など)
  - 最小単位にあわせた位置情報へ変換
- **解析**
  - 統計
  - 傾向の算出など
- **情報可視化**
  - 地理的情報表現
  - プリズムマップ化



可視化システムの説明 – 詳細(1/2)

- **可視化対象データ**
  - 3_log内の2009年5月～2010年4月の各ファイル
  - 下記の2パターンそれぞれについて分類して可視化

	Push型マルウェア	Pull型マルウェア
特徴	外部PCからマルウェアを待ちうけさせる	外部PCへマルウェアを取得させる
図解		

- **地理情報への変換**
  - MaxMind社のGeoIP
    - IPアドレスから地理情報（緯度/経度・国・県等）へ変換するシステム

MWSデータ

↓

地理情報変換

↓

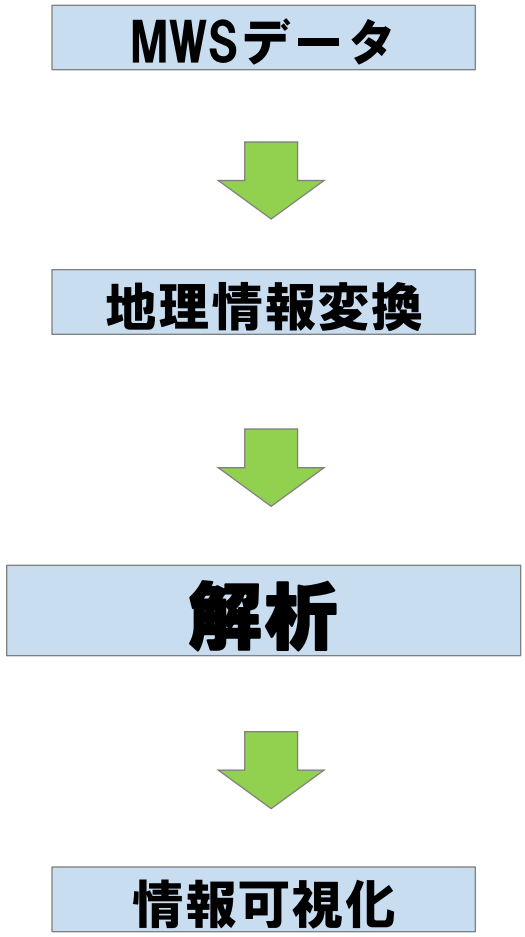
解析

↓

情報可視化

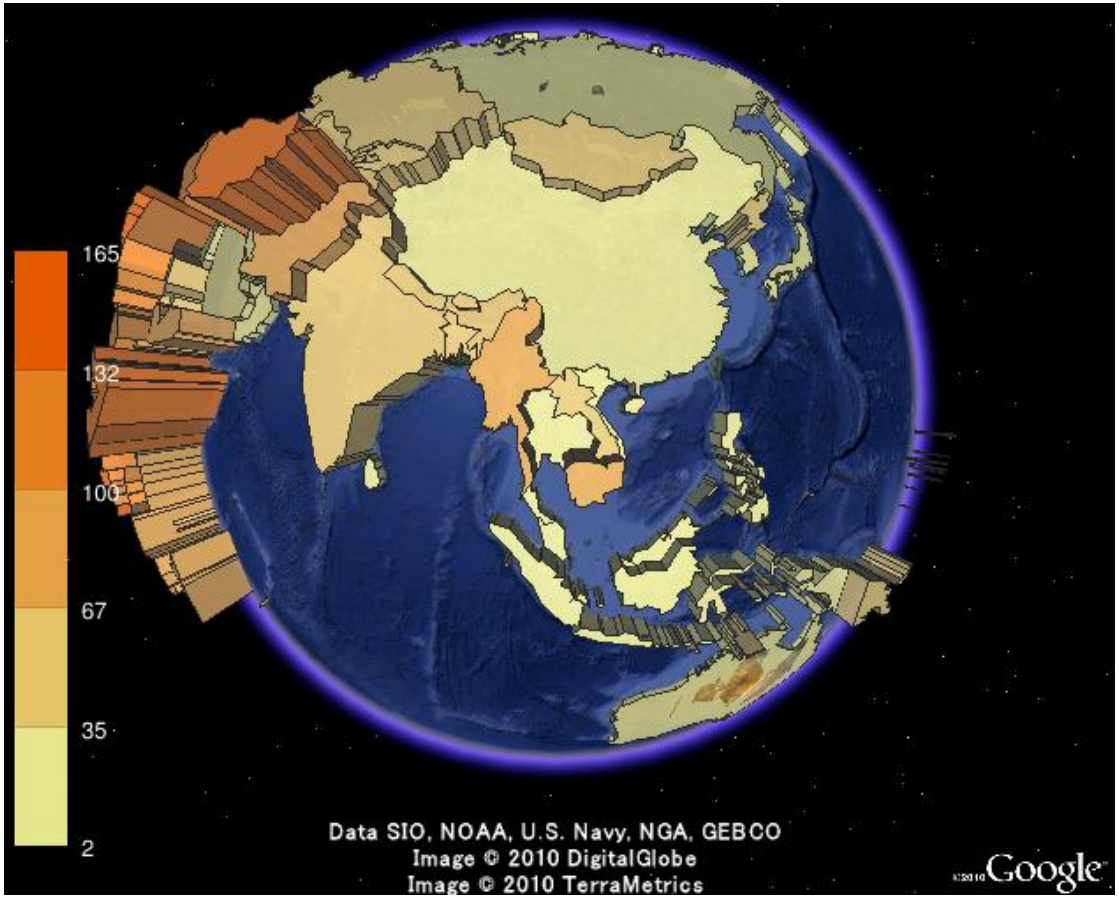
可視化システムの説明 – 詳細(2/2)

- **時系列表現**
  - 一日毎に統計を取得して描画
  - 日付を進む/戻ることができる
- **詳細情報の表示**
  - 該当日の攻撃があった順番に表示する
  - 送信元/先IPアドレス、時刻等
- **実行環境への配慮**
  - Google Earthさえあれば実行可能
  - Webシステムへの組み込み可能



可視化システムの説明 – プリズムマップ

- 地域別にポリゴンを生成して描画する方式
  - 高さ・色が通信量を表現
- 黄色(0件)から通信量に応じて赤く描画した



MWSデータ

↓

地理情報変換

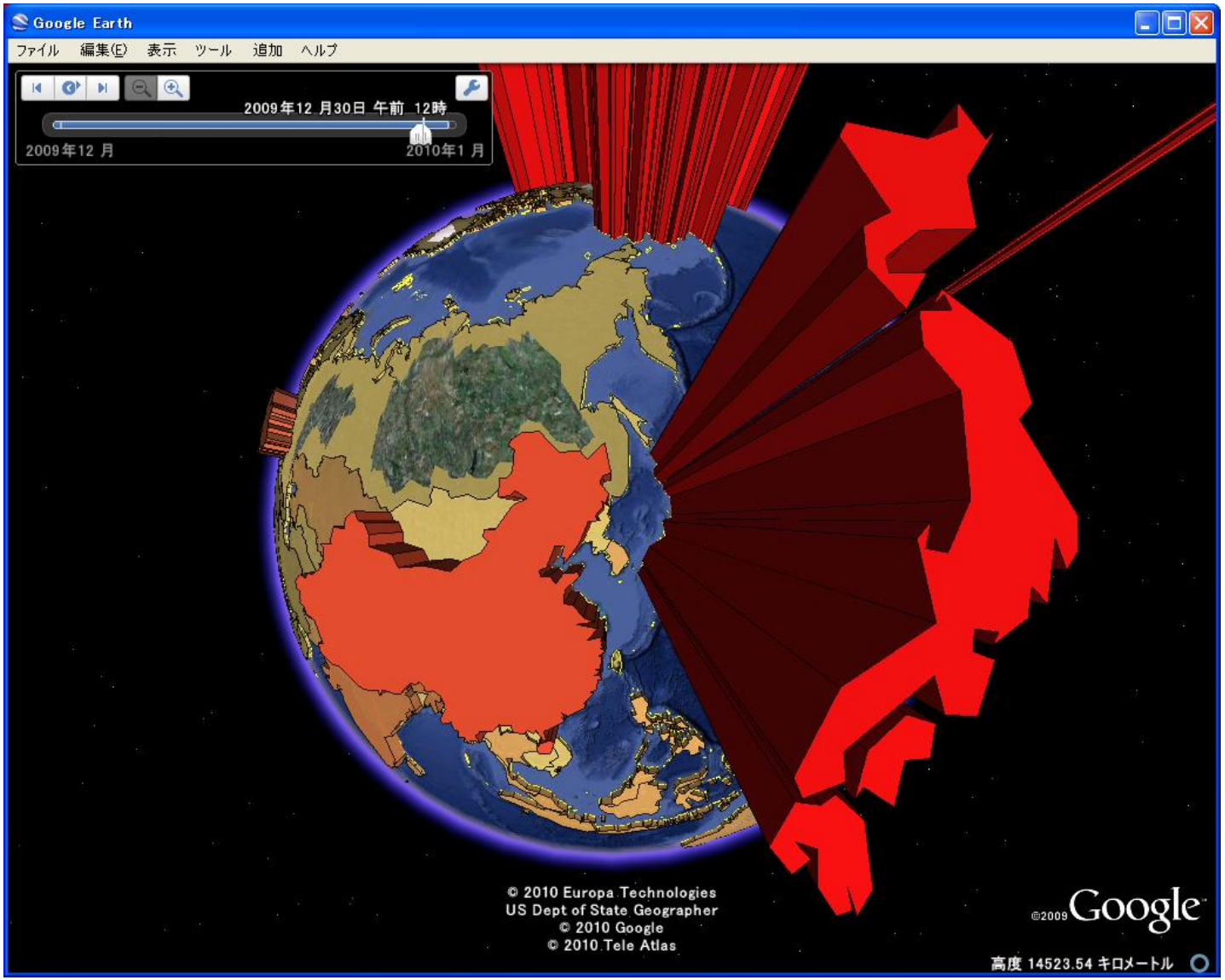
↓

解析

↓

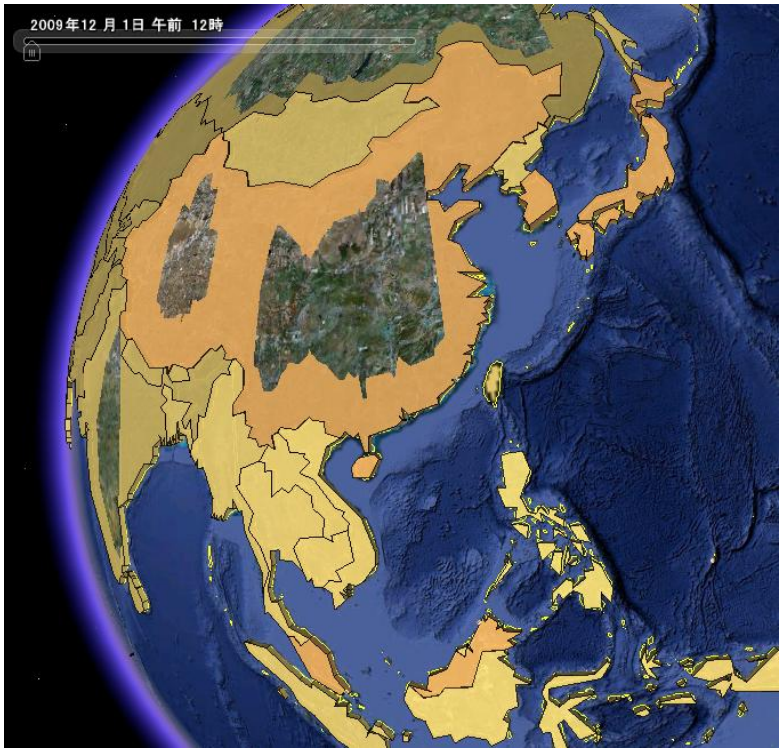
情報可視化

デモ

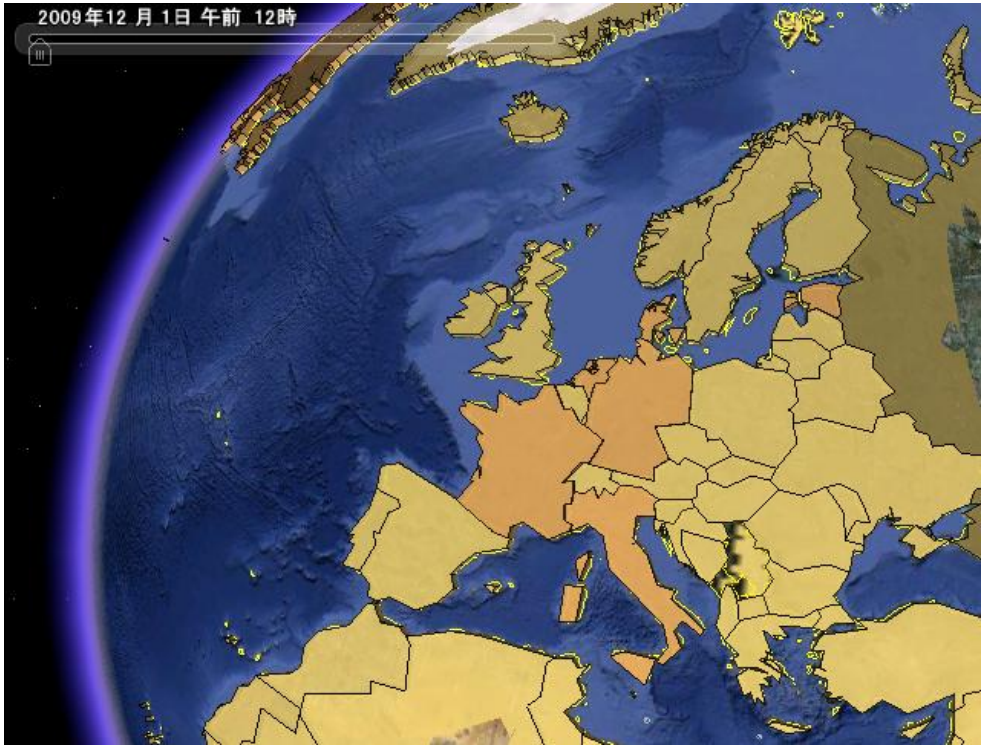


可視化結果 – Push型

- 1年間で約4万件のデータ
- アジア、欧州、欧米に散布
- 一日につき多くても20件程度の通信



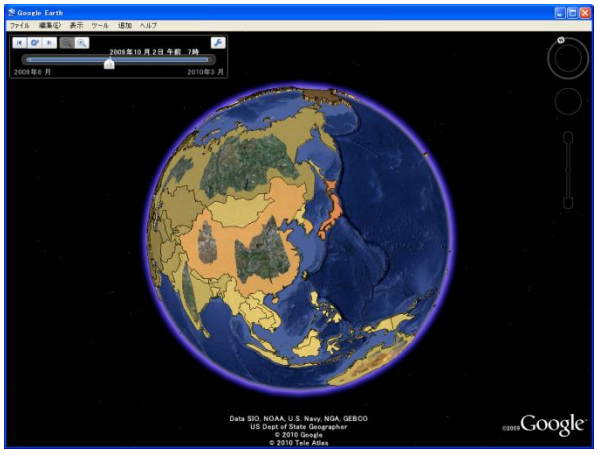
アジアの例



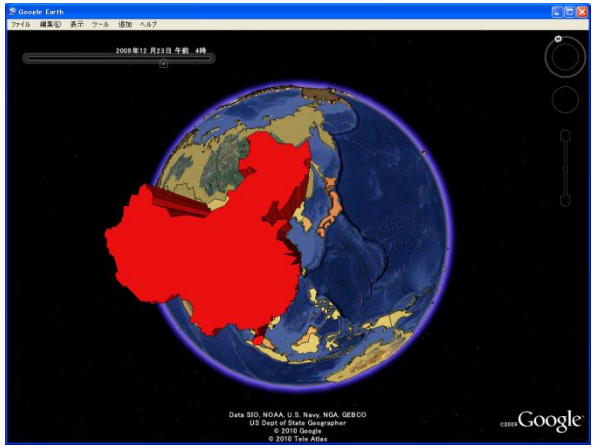
欧州の例

可視化結果 – Push型

- 2009年5月1日～2009年12月10日
  - 中国、日本、欧米など各国から
    平均1～5件程度の通信
- 2009年12月11日～2010年1月4日
  - 中国から平均450件/日の通信が行われていた
  - 期間中の中国のみの通信で12000件
  - ほぼ単一IPからの攻撃(11790件)
- 2010年1月5日～2010年4月30日
  - 世界各国から少量の通信
    平均1～5件/日程度に戻る



可視化例 – 2009/10/2



可視化例 – 2009/12/23

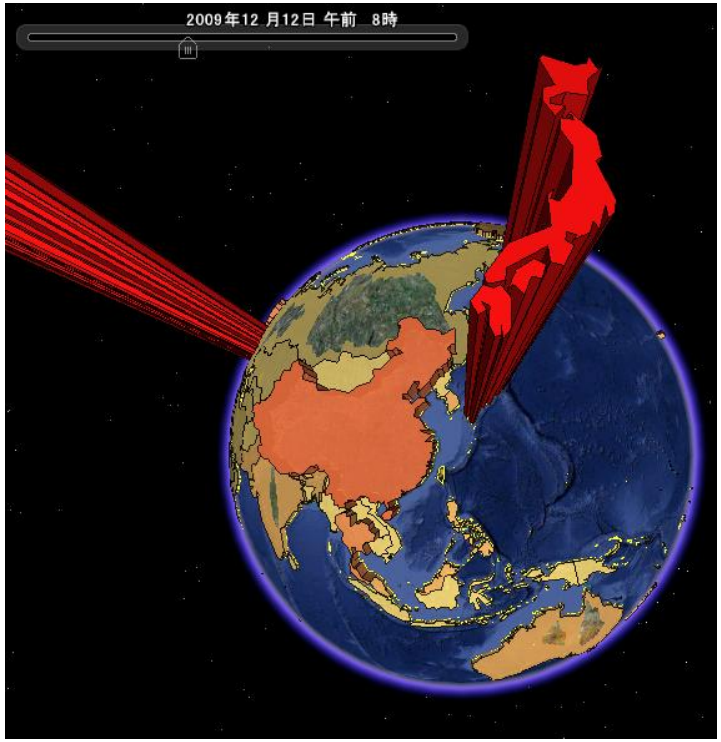
可視化結果 – Push型の中国の通信

- 2009年12月11日～2010年1月4日　中国からの通信
- Unknownは他ベンダーでWormやSpybotと判定されている

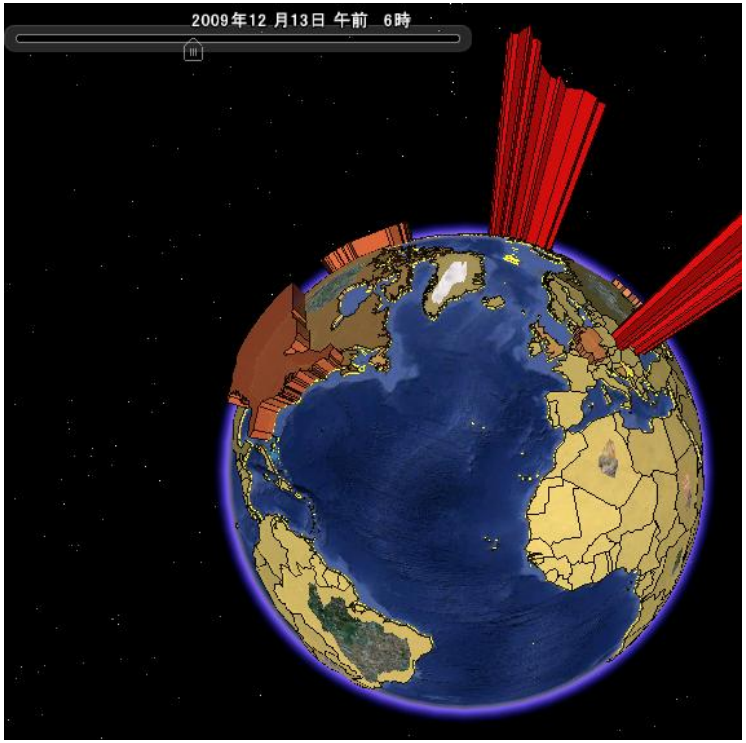
検体名	検知数
WORM_SPYBOT.AWS	9234
Unknown	1385
WORM_SPYBOT.BDS	1171
（以下は検体名とハッシュ値がばらばら）	
WORM_ALLAPLE.IK	20
WORM_ALLAPLE.AC	4
PE_VIRUT.AV	4
PE_VIRUT.AT	3
TROJ_AGENT.VW	1
PE_VIRUT.ABY	1

可視化結果 – Pull型

- Pull型データ1年分はおよそ110万件
- アジア、欧州、欧米に散布 – 欧州は若干少ない
- 日本は常時通信量が多い



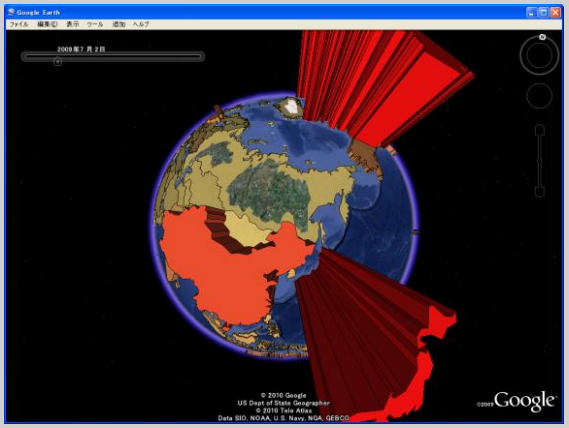
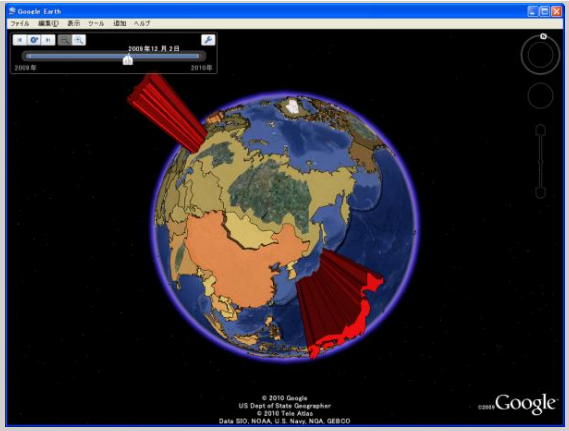
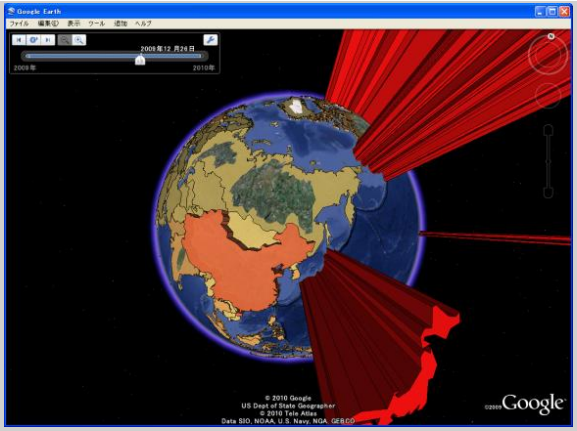
アジアの例



欧州・欧米の例

可視化結果 – Pull型

- カナダ　→　ウクライナ　→　アメリカへの通信量の遷移
- 攻撃の時間的関係が同じ（同一時刻にUnknownと特定検体通信）

	～2009年12月1日	2009年12月2日～25日	2009年12月26日～
全体			
詳細			

honey069	67.215.1.206	2009-12-01 00:04	TROJ_BUZUS.BEZ
honey069	67.215.1.206	2009-12-01 00:04	UNKNOWN
honey069	67.215.1.206	2009-12-01 00:05	TROJ_BUZUS.BMH
honey019	67.215.1.206	2009-12-01 00:05	UNKNOWN
honey019	67.215.1.206	2009-12-01 00:05	TROJ_BUZUS.AQP
honey019	67.215.1.206	2009-12-01 00:05	UNKNOWN
honey019	67.215.1.206	2009-12-01 00:06	TROJ_BUZUS.BMH

honey080	91.207.7.116	2009-12-03 12:50	UNKNOWN
honey080	91.207.7.116	2009-12-03 12:50	TROJ_BUZUS.BMH
honey080	91.207.7.116	2009-12-03 12:50	UNKNOWN
honey053	91.207.7.116	2009-12-03 12:51	TROJ_BUZUS.BMH
honey053	91.207.7.116	2009-12-03 12:51	TROJ_BUZUS.BMH
honey053	91.207.7.116	2009-12-03 12:51	UNKNOWN
honey053	91.207.7.116	2009-12-03 12:51	UNKNOWN
honey053	91.207.7.116	2009-12-03 12:51	TROJ_BUZUS.BEZ
honey053	91.207.7.116	2009-12-03 12:51	UNKNOWN

honey076	98.126.47.46	2009-12-26 00:02	TROJ_BUZUS.BEZ
honey076	98.126.47.46	2009-12-26 00:02	WORM_KOLAB.EA
honey076	98.126.47.46	2009-12-26 00:02	WORM_KOLAB.EA
honey059	98.126.47.46	2009-12-26 00:02	TROJ_BUZUS.BEZ
honey059	98.126.47.46	2009-12-26 00:02	WORM_KOLAB.EA
honey059	98.126.47.46	2009-12-26 00:02	WORM_KOLAB.EA

可視化結果 – Pull型マルウェア通信例

カナダの通信例

TROJ_MALWARE.VTG	222
TROJ_BUZUS.AQP	79
TROJ_BUZUS.BEZ	61
TROJ_BUZUS.BMH	17
WORM_ALLAPLE.AC	1

TROJ_MALWARE.VTGは
検出時点ではUNKNOWNの検体
後に判明した名前で記載

ウクライナの通信例

WORM_KOLAB.EA	983
TROJ_BUZUS.BEZ	483
TROJ_MALWARE.VTG	241
UNKNOWN	36

カナダの検体のハッシュ値は
TROJ_MALWARE.VTGと一致
TROJ_BUZUS.BEZとも一致

時期が後になると
WORM_KOLAB.EZが増える
TROJ_BUZUS.BEZのハッシュ値
が変わる

アメリカの通信例

WORM_KOLAB.EA	1036
TROJ_BUZUS.BEZ	868
TROJ_MALWARE.VTG	475
UNKNOWN	42
WORM_ALLAPLE.IK	6
その他	5

ウクライナの検体ハッシュ値
後半のTROJ_BUZUS.BEZと一致
WORM_KOLABも一致

UNKNOWNは一致しない

まとめ

- 可視化システムを実装し、Push型Pull型マルウェアの特徴把握を行った

  - Push型
    - 全体的に1～5件/日程度のデータ通信を行う国が多かった
    - 12月中旬は中国からの特徴的通信が見られた
      - バンクーバーオリンピックなどの時期と重なるが詳細不明

  - Pull型
    カナダ→ウクライナ→アメリカと推移していると思われる通信がある
    - ボットネットのハーダーがダウンロード対象サーバーを変更などの理由が考えられる
      - 対セキュリティ対策？

  - 双方に見られる特徴
    - 攻撃量が突然多くなる等の新規のウイルス感染を広げようとする活動では、当たり前のように未知検体を用いることが多い
      - 未知検体の利用
      - 未知検体が既知検知となったとき、他の未知検体へ変更する動きもみられた