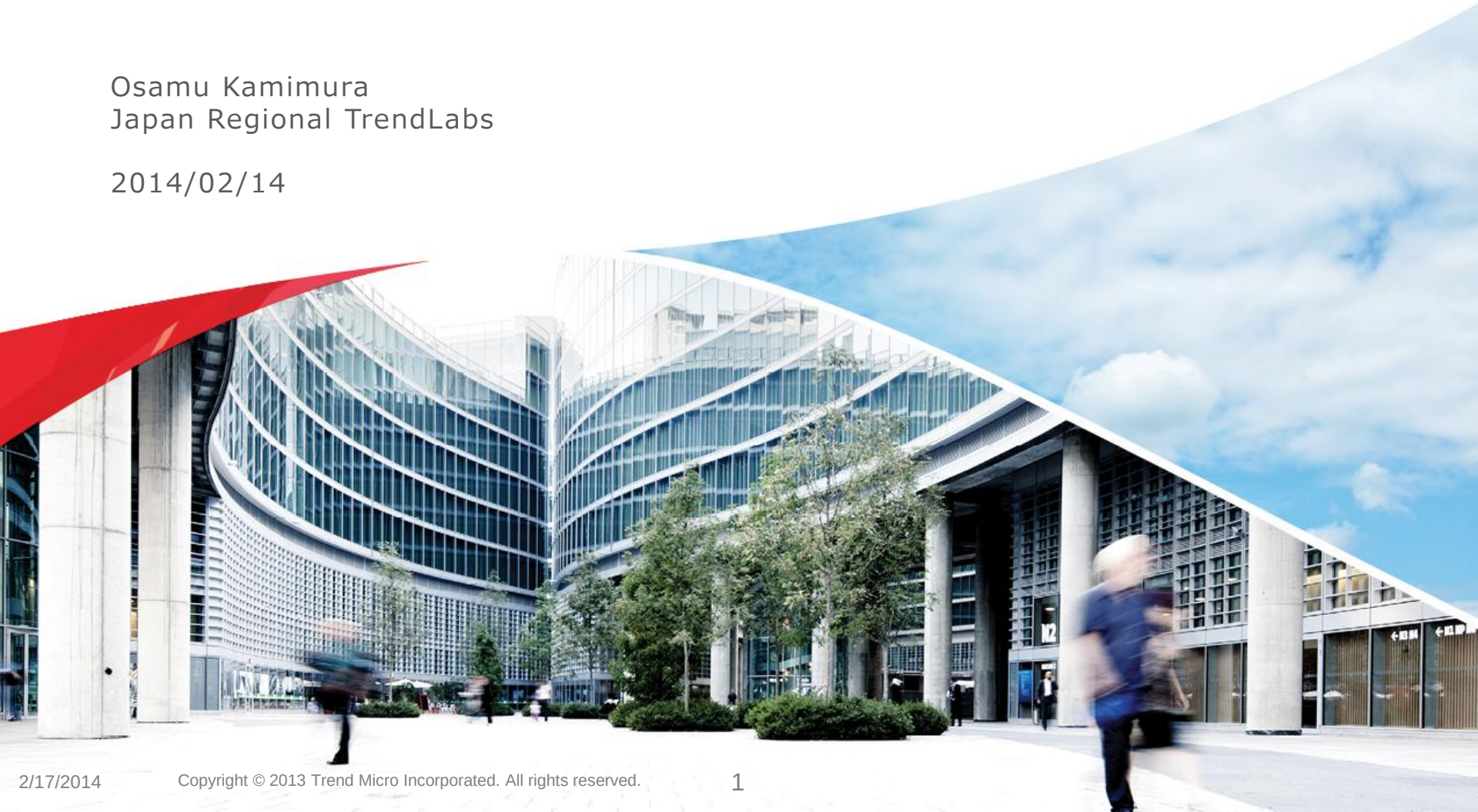
IAjapan 第10回 迷惑メール対策カンファレンス

スパムメール×マルウェアの実態

Osamu Kamimura
Japan Regional TrendLabs

2014/02/14



世界2拠点のTrendLabs / 10拠点のRegional TrendLabs

24時間365日体制のウイルス解析・サポートセンター

- ウイルス解析＆パターンファイル作成
- トレンドマイクロ エキスパートサービス 運用監視センター
- カスタマーサポート

世界１０拠点、 1200人以上のスタッフで構成
= フィリピン(マニラ)、日本、台湾、中国（上海）、アメリカ（テキサス）、
アイルランド、ドイツ、フランス、メキシコ、ブラジル

昨今のメディア報道

アカウント盗まれ不審メール大量送信　農研機構と生物研　茨城

2014.1.22 02:51

つくば市の農業・食品産業技術総合研究機構（農研機構）と農業生物資源研究所（生物研）は２１日、研究員がメールを利用するための情報（アカウント）を盗まれ、不審なメールが大量に送信されていたと発表した。

農研機構によると、昨年１２月３１日に男性研究員（３５）のアカウントを使った不審ルの大量送信が判明。研究員が同２５日以降にフィッシングメールに書かれたサイクセスし、ＩＤとパスワードを入力したことが原因とみられる。

研でも今年１月６日、不審なメールの大量送信が発覚。メールには、英文で「事業トナーを探しています」などと書かれ、連絡先メールアドレスも記載されていた。

機構、生物研ともに盗まれたアカウントを使用停止にしており、これまでに個人情の漏洩（ろうえい）は確認されていないという。

※MSN産経ニュース

ドイツで約1600万人分のアカウント情報流出---海外メディアの報道

2014/01/22
鈴木 英子＝ニューズフロント （筆者執筆記事一覧）

記事一覧へ >> シェア いいね！ 8 ツイート 40 +1 1 B! 6

ドイツでインターネットユーザー約1600万人分のアカウント情報流出が確認されたと、複数の海外メディア（Financial Times、Guardian、CIO.comなど）が現地時間2014年1月21日に報じた。

ドイツ情報技術安全局の発表によると、複数のコンピュータが不正なソフトウエアに感染し、電子メールアドレスやパスワードが盗まれた。約半数の電子メールアドレスの末尾に「.de」がついていることから、被害者の多くがドイツ人と見られる。

現在、警察当局と専門家が攻撃の範囲などを調査しており、攻撃は長期間にわたって行われていたもようで、犯罪組織による犯行と考えられる。

情報流出は当局がボットネットを調査している中で見つかった。しかし情報技術安全局広報担当者は「背景について説明することはできない」として、どのボットネットが関連していたかなどについては明らかにしなかった。

※ITPro by 日経コンピュータ

実際にあったお問い合わせ

メールが勝手に大量送信されているようだ

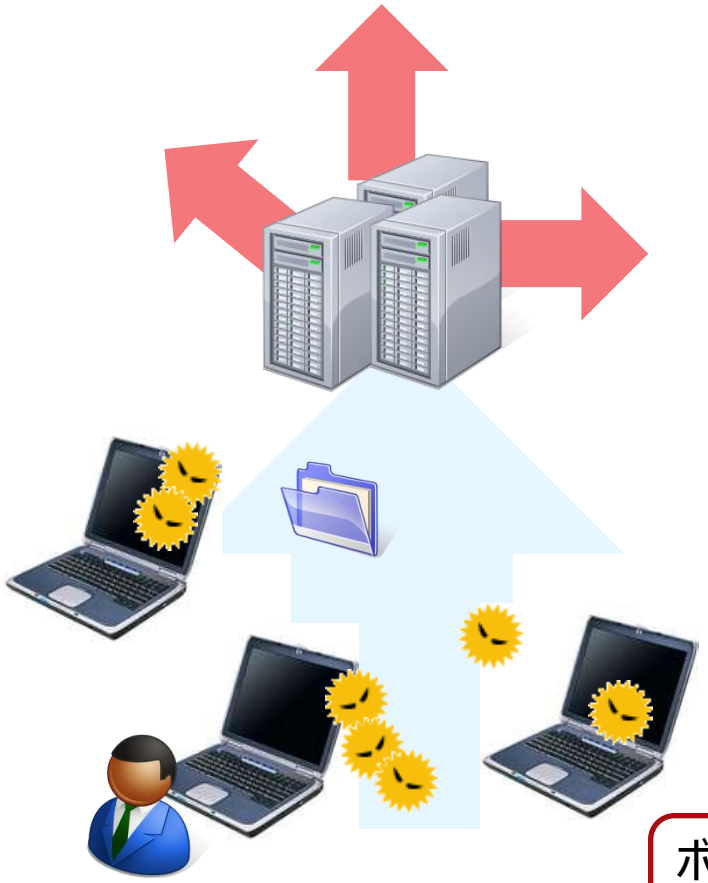
1台のクライアントからメールを大量に送信する現象が発生
アドレス帳の登録に対してではなく、gmail などのフリーメールに対して手当たり次第に送信されていた模様

ウイルスに感染したらしく、プロバイダーからスパムメールが大量に発信されているとの連絡を受けた

ユーザが気づかないうちにメールが送られており、通知によってはじめて気づくパターンが多い

マルウェア×スパムメール　配信

- ウイルス感染により、スパムメールを配信しているパターン



添付メールやWebから感染する
　イベントに便乗した攻撃が多い
　クリスマス、正月、バレンタインなど
ユーザがクリック/Webページにアクセスしてしまうことで感染

感染後は攻撃者からあらゆるコマンド操作が可能に

スパムメール送信、メールアドレス収集など

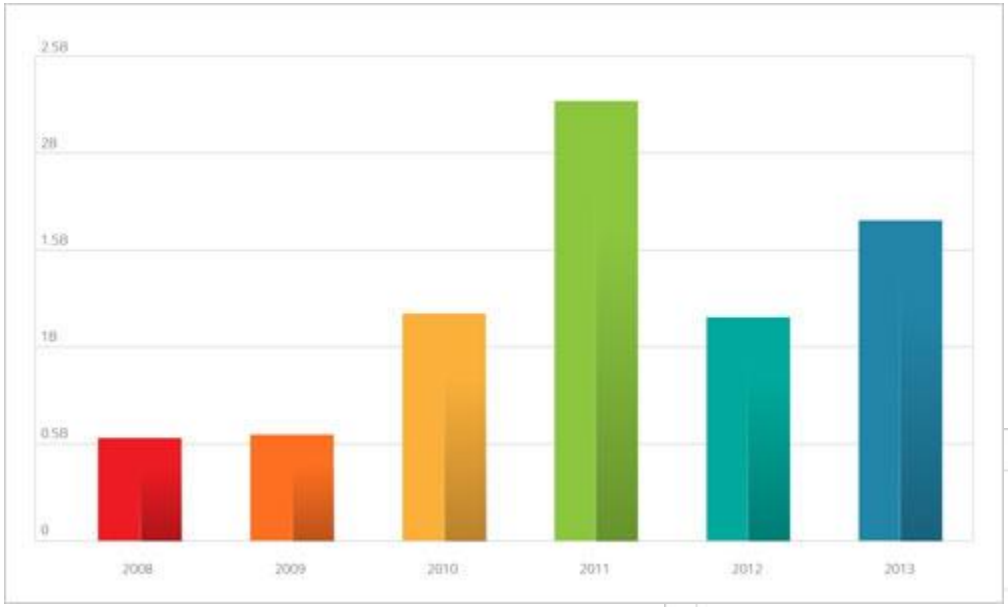
ボットネットを形成し、一度で大量のメールの送信も可能に
また、動作後は削除されて消えてしまうことも

マルウェア×スパムメール　受信

- スパムメールと共にウイルスが添付されているパターン

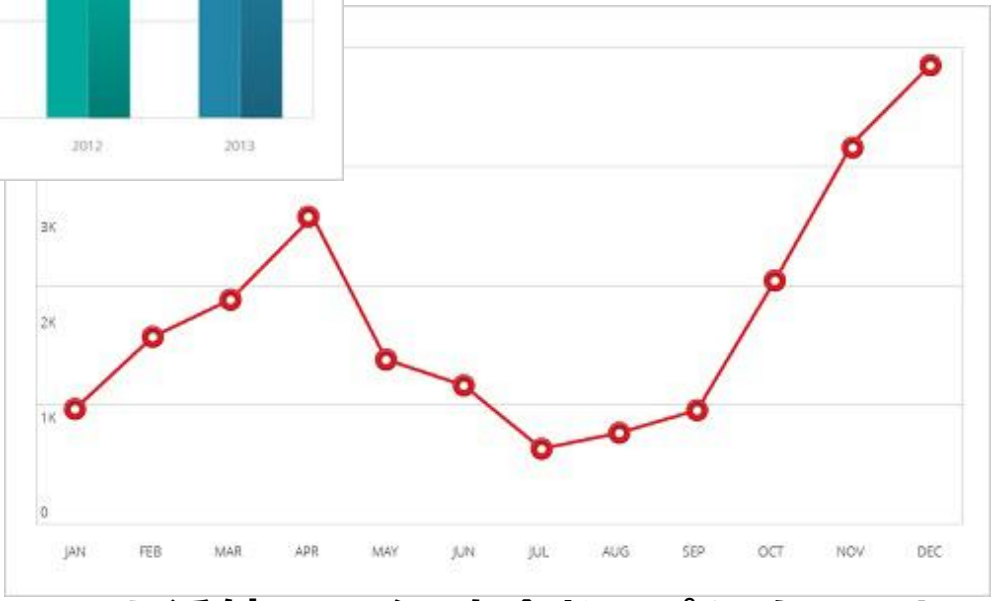
- 最近ではスパムメールにUPATREが添付されているケースを多く確認

スパムメール数の推移



スパムメールの総数は
2012年に比べて増加

- 特に健康に関するスパムメールの増加を確認
- 200万通以上が確認された時期も



不正な添付ファイルを含むスパムメールは
9月から12月にかけて急激に増加

まとめ

- アカウント流出の被害が増加
- マルウェアが関連したスパムメールが多く存在
- 感染していても気づかないユーザが多い

不審なファイルは触らない
不審なサイトへアクセスしない

Thank You