TREND MICRO
Securing Your Journey to the Cloud

トレンドマイクロにおける スレットリサーチの現状と課題

松川 博英

シニアリサーチャー

Forward-looking **T**hreat **R**esearch

2012年10月31日

会社概要

会社名	トレンドマイクロ株式会社 代表取締役社長 兼 CEO　エバ・チェン　（陳　怡芬）
所在地	東京本社　　東京都渋谷区代々木2-1-1新宿マインズタワー
設立	1989年10月24日
資本金	183億8,600万円（2011年12月末）
株式情報	東京証券取引所市場第１部　証券コード：4704　トレンド
営業品目	コンピュータ及びインターネット用 セキュリティ関連製品・サービスの開発・販売
社員数	4,942名　（2011年12月末）
売上高	963億9,200万円　（2011年12月末）
海外子会社	米国、カナダ、アイルランド、フランス、ドイツ、イタリア、英国、スイス、オーストラリア、中国（上海）、中国（香港）、中国（北京）、インド、韓国、マレーシア、シンガポール、台湾、タイ、ブラジル、メキシコ、ニュージーランド

代表取締役兼CEO
エバ・チェン

取締役副社長
日本地域担当兼アジア・ラテンアメリカ地域営業推進担当
大三川 彰彦

Our **Vision**

A world safe for exchanging digital information

デジタル情報を安全に交換できる社会

自己紹介

松川 博英 （MATSUKAWA Bakuei）

シニアリサーチャー
Forward-looking Threat Research

1997年、トレンドマイクロ入社。テクニカルサポートチームリーダーとしてウイルスバスターやInterScan VirusWallなどの製品テクニカルサポート、およびウイルスインシデントサポートに従事した後、2007年、地域に特化した脅威への対応を専門に行う「Regional TrendLabs」の設立に伴い、不正プログラムの解析を担当。解析チームリーダーとして、不正プログラムをコードレベルで詳細に解析した解析レポートの作成提供を主導。

2012年3月、先端脅威に関する調査/研究を専門に行うリサーチチーム「Forward-looking Threat Research」に異動し、世界で約20名のリサーチャーと共に活動。標的型攻撃/APTのエキスパートとして、LuckycatやIXESHEに関するリサーチペーパーの作成に関わるなど、主に標的型攻撃/APTに関する調査・研究に従事。

Forward-looking Threat Research teamとは

FTR の活動内容

- スレットインテリジェンス（Threat Intelligence）
  - セキュリティ脅威を完全に理解するために必要な全ての情報。良質なスレットインテリジェンスは、セキュリティ脅威に対抗するための判断・行動の助けとなる。

スレットリサーチとマルウェア解析

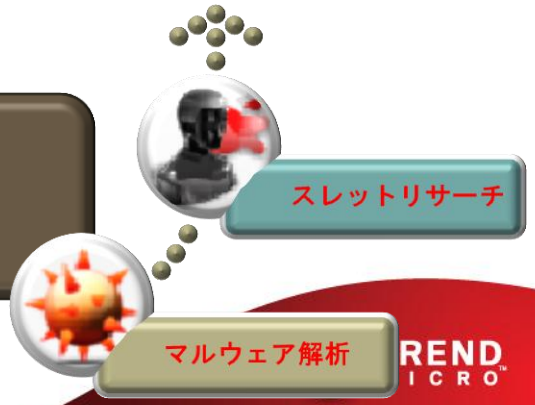
スレットリサーチ

- スレットインテリジェンスを得るために行われる全ての活動
- セキュリティ脅威に関する情報を収集・調査し分析することや、分析手法について研究することなど

マルウェア解析

- マルウェアの動作に関する事実情報を調べること
- マルウェアが手段に過ぎない現在の脅威では、マルウェア解析だけでは脅威の全貌は見えない

脅威の全貌を知るには、マルウェア解析を基礎として、攻撃全体の俯瞰や過去からの経緯を踏まえた攻撃者の目的や手法の傾向分析（スレットリサーチ）が必要



リサーチ例：PoisonIvyに関するリサーチ

8月 24

2012年上半期国内における持続的標的型攻撃の傾向レポートを公開

by マーケティングスペシャリスト - 森本 純

(1 投票, 平均値/最大値: 5.00 / 5, 評価済) ブックマークへ追加 7 users この記事を印刷

トレンドマイクロは、2012年上半期（1月～6月）日本国内における持続的標的型攻撃（Advanced Persistent Threats. APT）に関する傾向レポートを公開しました。

本レポートでは、2012年上半期（1月から6月）にかけてトレンドマイクロの日本国内に特化したリサーチ機関であるリージョナルトレンドラボが収集、分析した持続的標的型攻撃のサンプルを基に統計データをまとめています。また同時期に日本国内で最も顕著に使われていた攻撃ツールについて、よりプロアクティブな脅威動向分析を行うフォワードルッキングスレットリサーチが独自に行った分析も併せて紹介します。

レポート前半では、2012年上半期の事例報告の中で多く確認された標的型メールによる攻撃の各プロセスにおける「隠蔽」のテクニックを解説しています。

- 侵入・感染のプロセス：受信者が疑いにくい電子メールの添付ファイルとして侵入
  - ・メール添付ファイルの形式：67%が文書・画像ファイル（※1）
  - ・メールの偽装：組織内の会議情報など実在のメールの転用、メール不達時の自動応答メール、標的組織の取扱品の注文依頼、標的組織への履歴書送付の問い合わせに偽装した例を確認
- 情報の収集・窃取のプロセス：通常のWeb通信に見せかけた隠蔽工作
  - ・不正プログラム：38%が「BKDR_POISON」「BKDR_DARKMOON」（PoisonIvy）（※2）
  - ・通信ポート：60%がポート80、32%がポート443（※2）

※1：標的型攻撃に使用されたメールの添付ファイル100個を調査
※2：標的型攻撃に使用された不正プログラム50個を調査

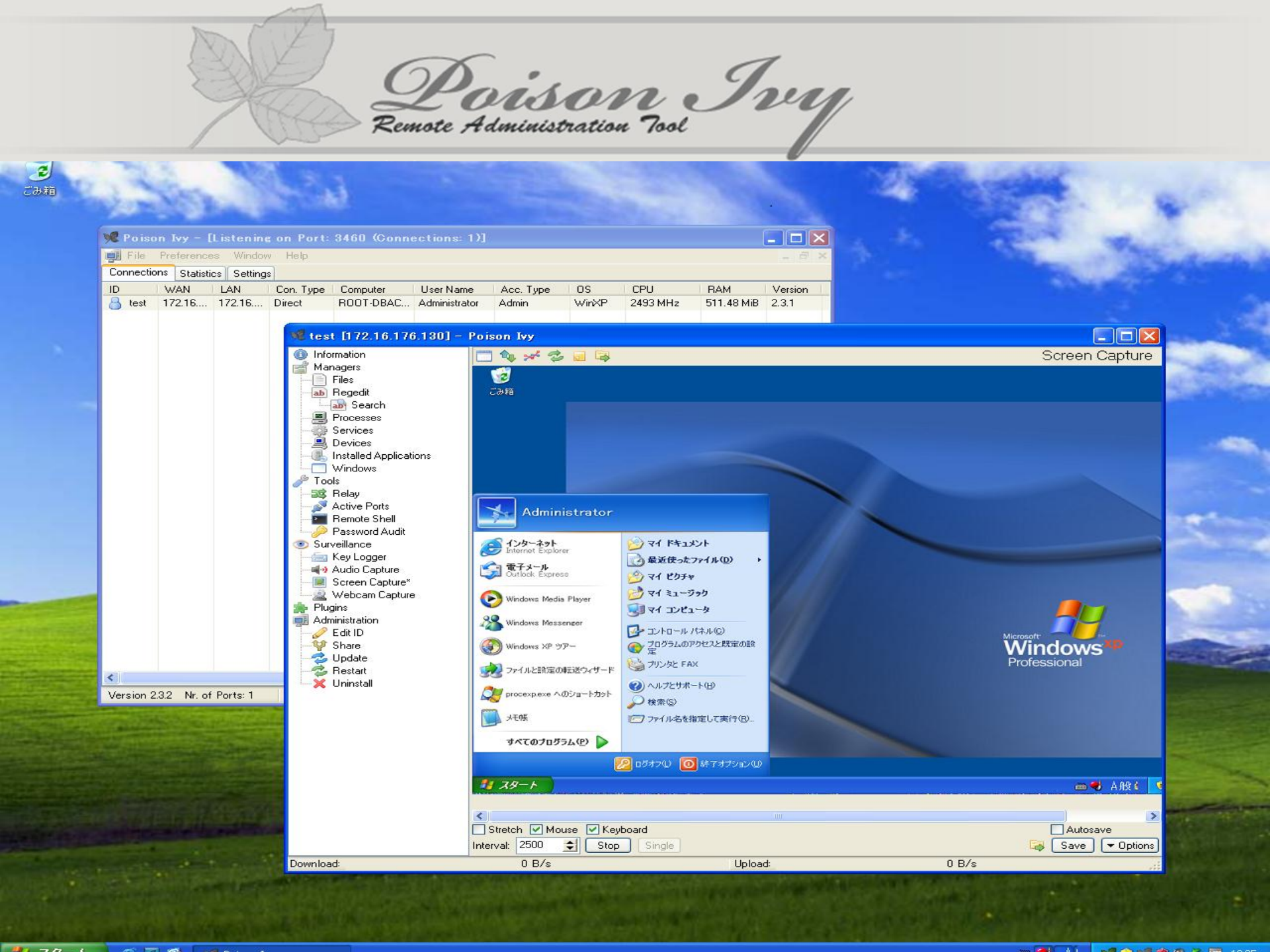
レポート後半では、2012年上半期の事例報告の中で、最も多く確認された不正プログラムであるPoisonIvyの攻撃使用時の共通点を分析し、単独の攻撃毎ではなく、一連の攻撃の「関連」を把握することで、その背後にある攻撃者グループの動向に着目し、持続的標的型攻撃への根本対策へつなげていく試みに関する調査結果を共有します。

- 2012年上半期に収集・抽出した50サンプルのうち、半数程度が同一の攻撃インフラを利用、また、少なくとも2009年からこのインフラが攻撃に利用されていたことを確認
- 巧妙化の一例として、標的組織のプロキシサーバ情報をハードコードしたサンプルを確認

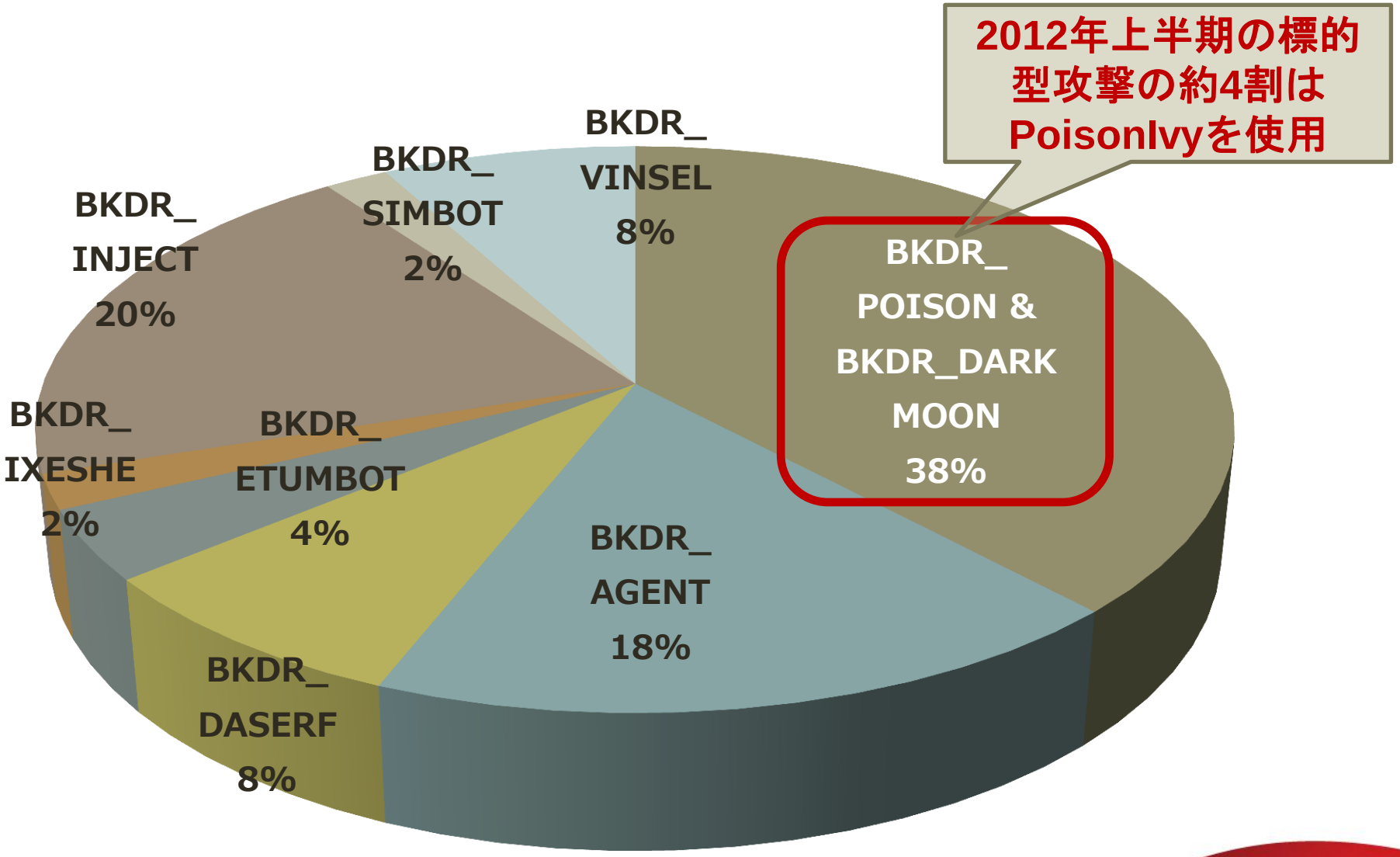
トレンドマイクロは、このような持続的標的型攻撃に対する調査を含め、サイバー攻撃に対する調査を継続して行うことで、よりプロアクティブな視点で、脅威やサイバー犯罪への対策の提供と対処に結びつくスレットインテリジェンスを提供していきます。

詳細については、以下からレポートをダウンロードしてご一読ください。

- 2012年上半期国内における持続的標的型攻撃（APT）の傾向レポートを公開
  https://inet.trendmicro.co.jp/doc_dl/select.asp?type=1&cid=81

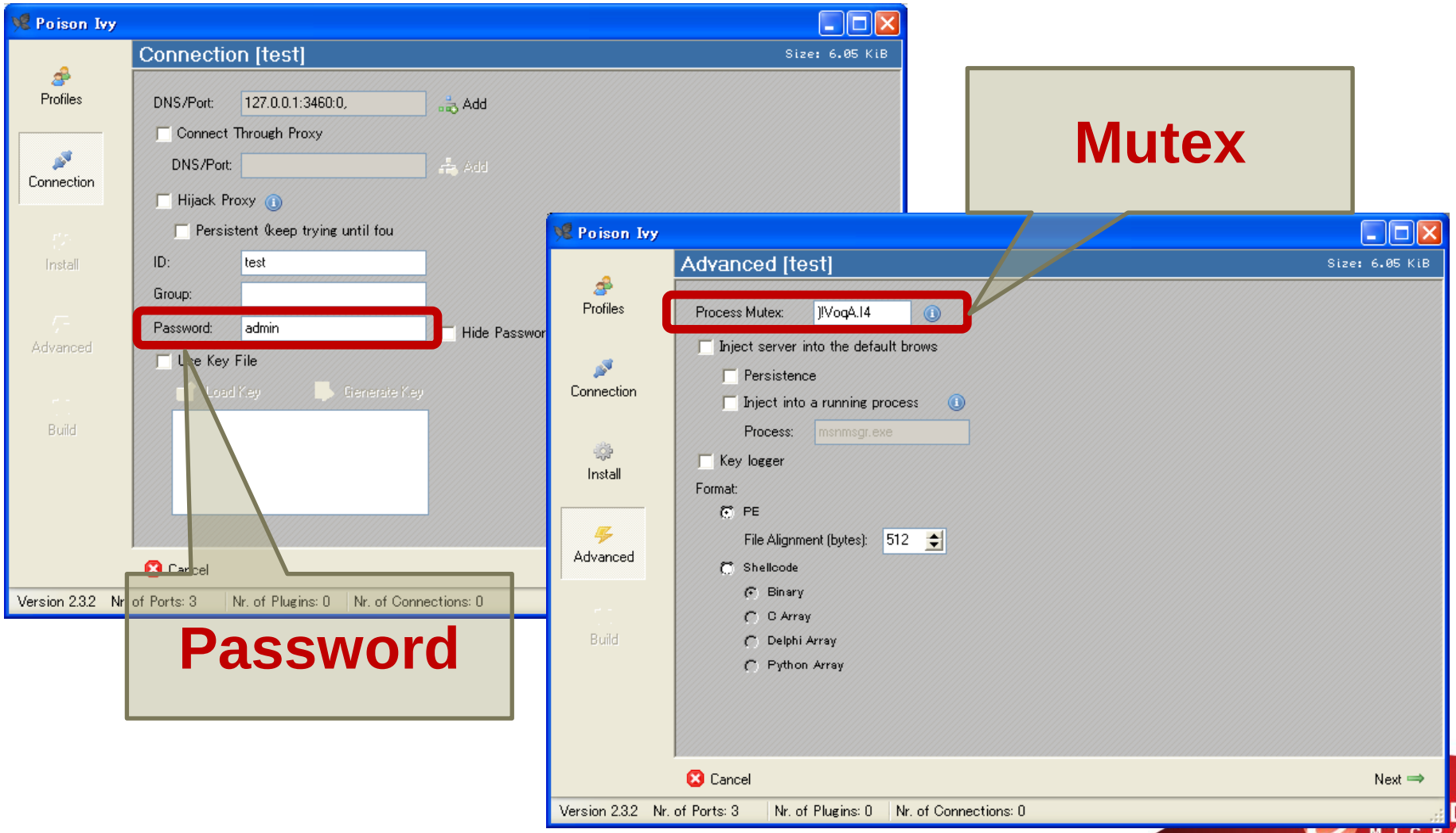

Poison Ivy
Remote Administration Tool
ごみ箱
Poison Ivy - [Listening on Port: 3460 (Connections: 1)]
File Preferences Window Help
Connections Statistics Settings
ID WAN LAN Con. Type Computer User Name Acc. Type OS CPU RAM Version
test 172.16.... 172.16.... Direct ROOT-DBAC... Administrator Admin WinXP 2493 MHz 511.48 MiB 2.3.1
Version 2.3.2 Nr. of Ports: 1
test [172.16.176.130] - Poison Ivy
Information
Managers
Files
Regedit
Search
Processes
Services
Devices
Installed Applications
Windows
Tools
Relay
Active Ports
Remote Shell
Password Audit
Surveillance
Key Logger
Audio Capture
Screen Capture*
Webcam Capture
Plugins
Administration
Edit ID
Share
Update
Restart
Uninstall
Screen Capture
ごみ箱
Administrator
インターネット Internet Explorer
電子メール Outlook Express
Windows Media Player
Windows Messenger
Windows XP ツアー
ファイルと設定の転送ウィザード
procexp.exe へのショートカット
メモ帳
すべてのプログラム(P)
マイ ドキュメント
最近使ったファイル(D)
マイ ピクチャ
マイ ミュージック
マイ コンピュータ
コントロール パネル(C)
プログラムのアクセスと既定の設定
プリンタと FAX
ヘルプとサポート(H)
検索(S)
ファイル名を指定して実行(R)...
ログオフ(L)
終了オプション(U)
Microsoft Windows XP Professional
スタート
Stretch Mouse Keyboard
Autosave
Interval: 2500
Stop Single
Save Options
Download: 0 B/s
Upload: 0 B/s

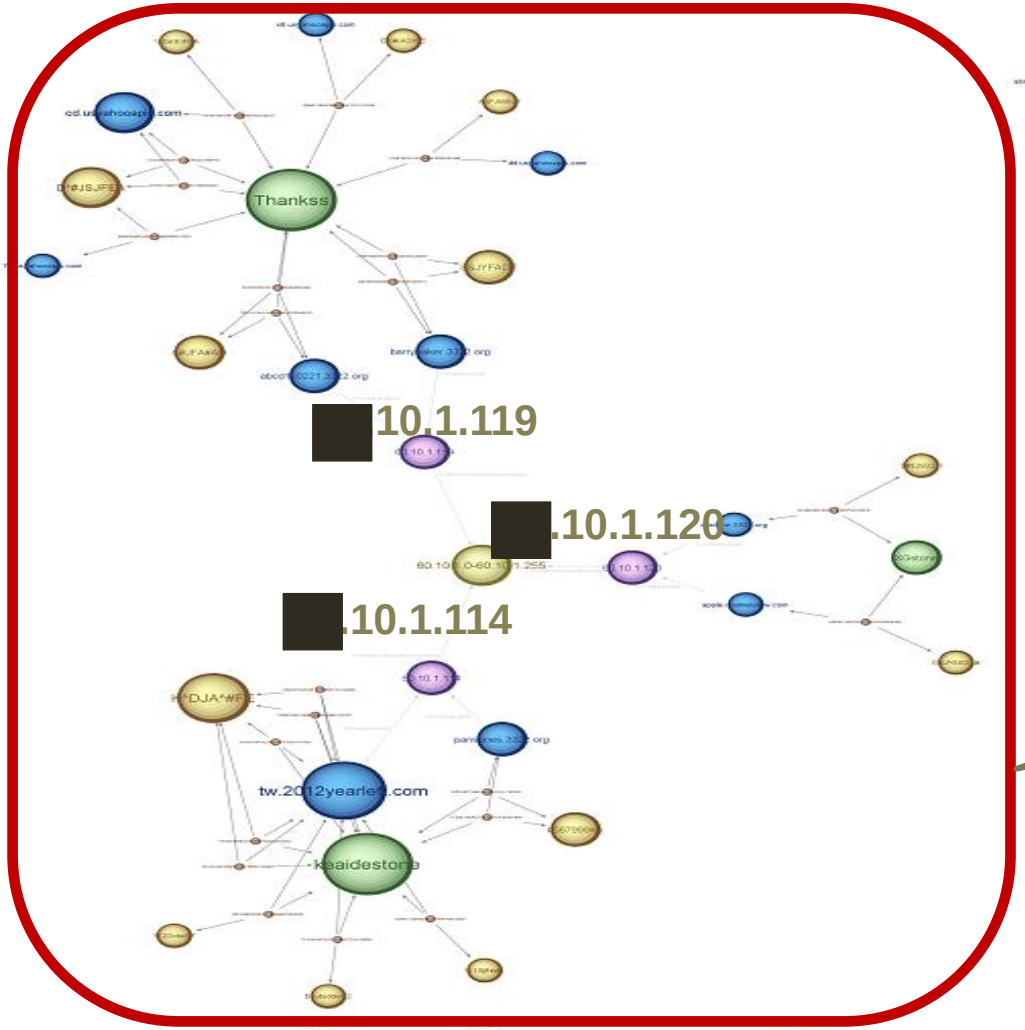
標的型攻撃でのPoisonIvyの使用

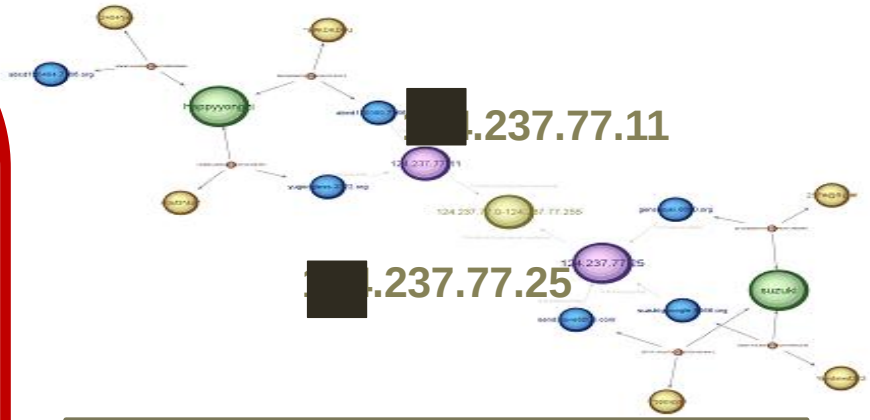


リージョナルトレンドラボ調べ・標的型攻撃メールに添付されていたバックドア（2012年上半期）

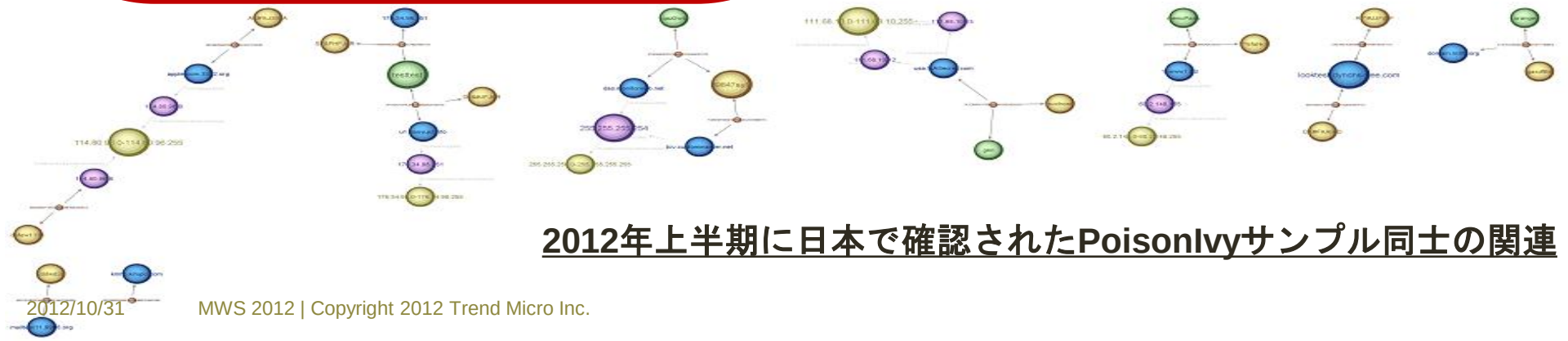
攻撃者を示す情報の存在







約5割は同じ攻撃者グループによる攻撃



2012年上半期に日本で確認されたPoisonIvyサンプル同士の関連

スレットリサーチの課題

- 法執行機関への協力とState Sponsored Cyber Attackへの中立性
- SPN（Smart Protection Network）に集まるビッグデータからのスレットインテリジェンスの創出


KNOW YOUR
ENEMY

TREND MICRO
Securing Your Journey to the Cloud

Q&A