CROUCHING YETI から見る 産業システム攻撃・諜報活動の高度化

株式会社カスペルスキー
ビジネスデベロップメントマネージャー
松岡 正人 (masato.matsuoka@kaspersky.com)

CROUCHING YETI：サマリー

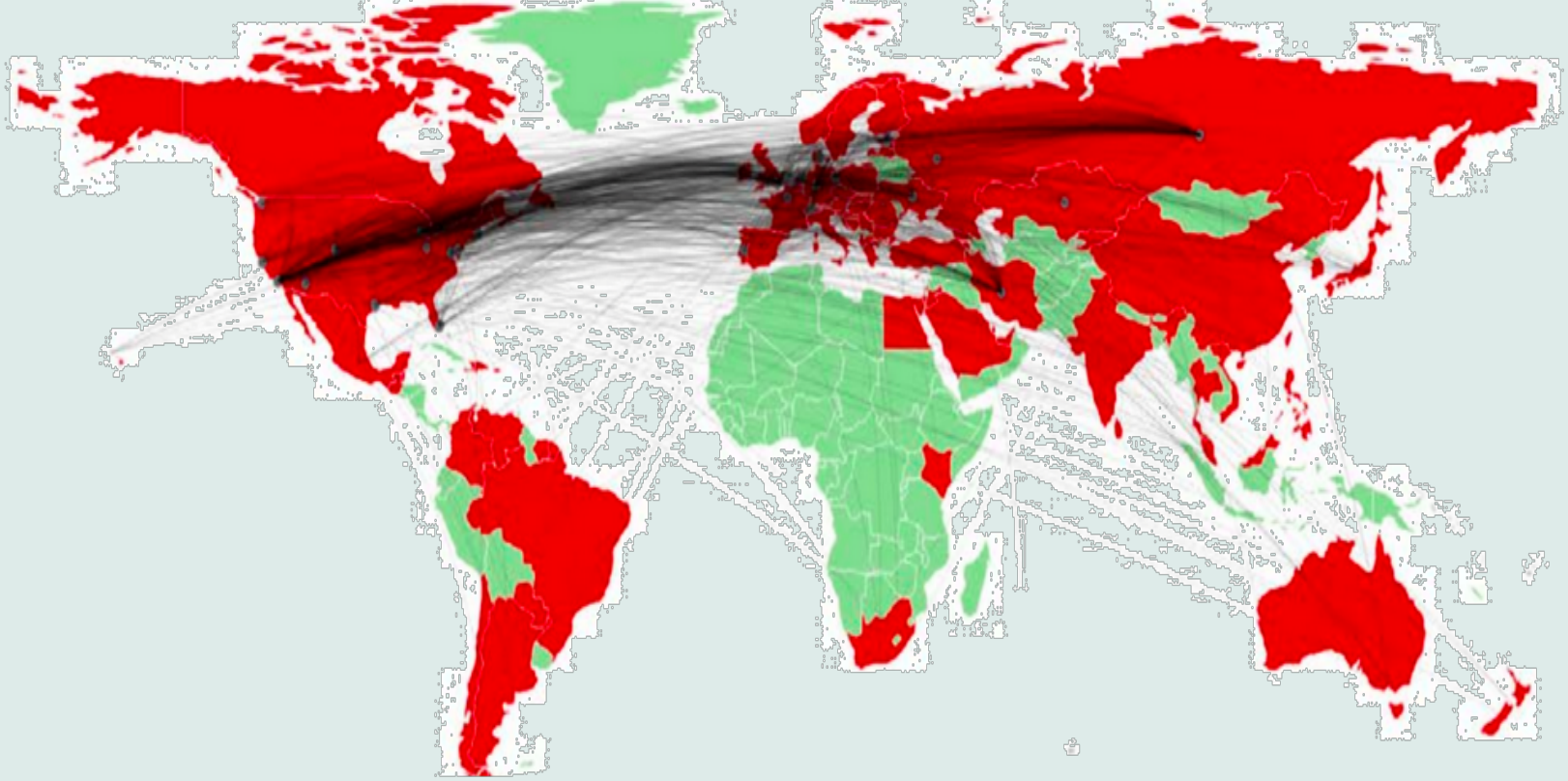
- 主な標的：非エネルギー分野
  - 産業 / 機械、製造、製薬、建設、教育、IT 関連
  - 被害者数は世界各地で 2,811、101 の組織、38ヶ国
  - 主にアメリカ、スペイン、日本、ドイツ、フランス、イタリア、トルコ、アイルランド、ポーランド、中国に存在する組織
  - 主な被害は企業秘密などの機密情報の流出
  - さまざまな分野を対象とした「幅広い調査活動」と定義することも妥当

CROUCHING YETI：サマリー

- 複数の追加モジュールを使用した攻撃
  - ゼロデイエクスプロイトは一切使わず、インターネット上で簡単に入手可能なエクスプロイトのみ使用
  - 最も多く使用されたツールは、トロイの木馬 Havex 、その亜種を合計 27 種類、さらに複数の追加モジュールを発見
  - 産業用制御システムからのデータ収集を目的とするツールが2種、OPC スキャナーモジュール とネットワークスキャンツール
  - ツールは UTC 時間の 6 時から 16 時の間にコンパイル、西ヨーロッパと東ヨーロッパの各国がこの時間帯に合致

CROUCHING YETI：サマリー

- “Bear” ではなく “Yeti”
  - 攻撃者の言語を分析した結果、キリル語（またはキリル語の別言語への音訳）は一切認められませんでした
    - Red October、Miniduke、Cosmicduke、Snake、TeamSpy の調査結果にはキリル語が含まれていた
  - ネイティブによって書かれたものではないと思われる英語で、フランス語やスウェーデン語の使用を示す手がかりも見つかっている
  - Energetic Bearは、Crowd Strike 社がつけた名前。同社 はこの活動の拠点はロシアにあるとしており、その属性から Bear と命名
  - 弊社の調査ではロシア圏の証拠が見つかっていないため、よりミステリアスなYeti（イエティ：雪男）と命名



雪男の足跡

YETI : TOP BEER IN COLORADO!

*http://greatdivide.com/

KASPERSKY lab

被害者の内訳

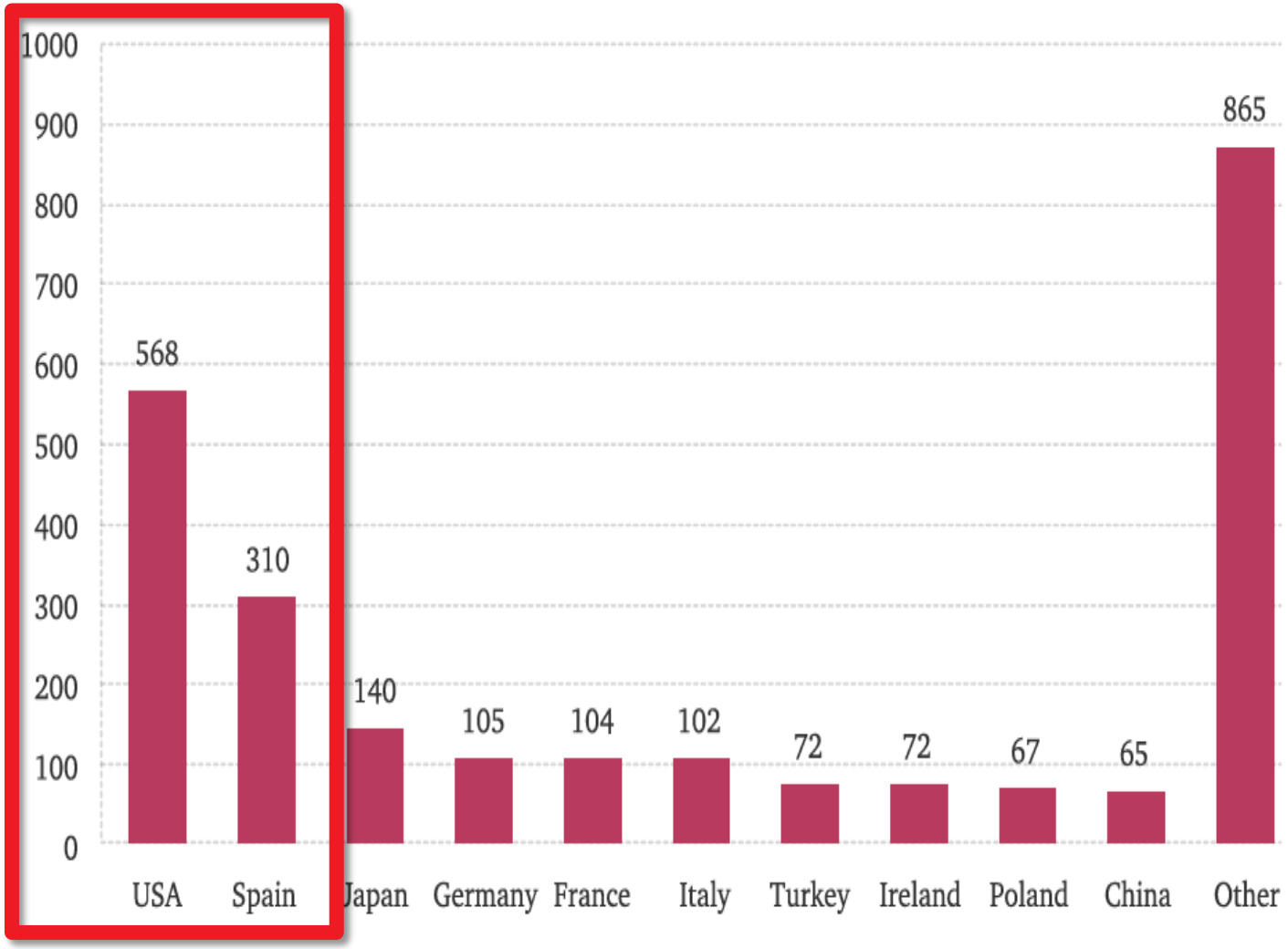
- 2,811の被害者のうち101社の属性
  - 精密射出成形関連メーカー
  - 医薬品卸し
  - 建設会社
  - ウェブデザイン・コンテンツ開発会社
  - 大学
  - 大手機械メーカー
  - 医薬品、自動車、印刷業向け機械メーカー
  - 建設機械、エネルギーシステム卸し
  - IT製品・サービス販売代理店
  - 電機電子・IT製品卸し
  - データセンター
  - システムインテグレーター
  - 検査装置メーカー
  - SCADAシステムメーカー

など

業種	特定被害台数
教育	32
調査・研究	14
機械	10
情報処理	10
建設	9
政府・自治体	8
健康・医療	5
ネットワークインフラ	3
製薬	2
電機	2
包装	2
金融	2
エネルギー	2
清掃	1
自動車	1
土木	1
運輸	1
化学	1

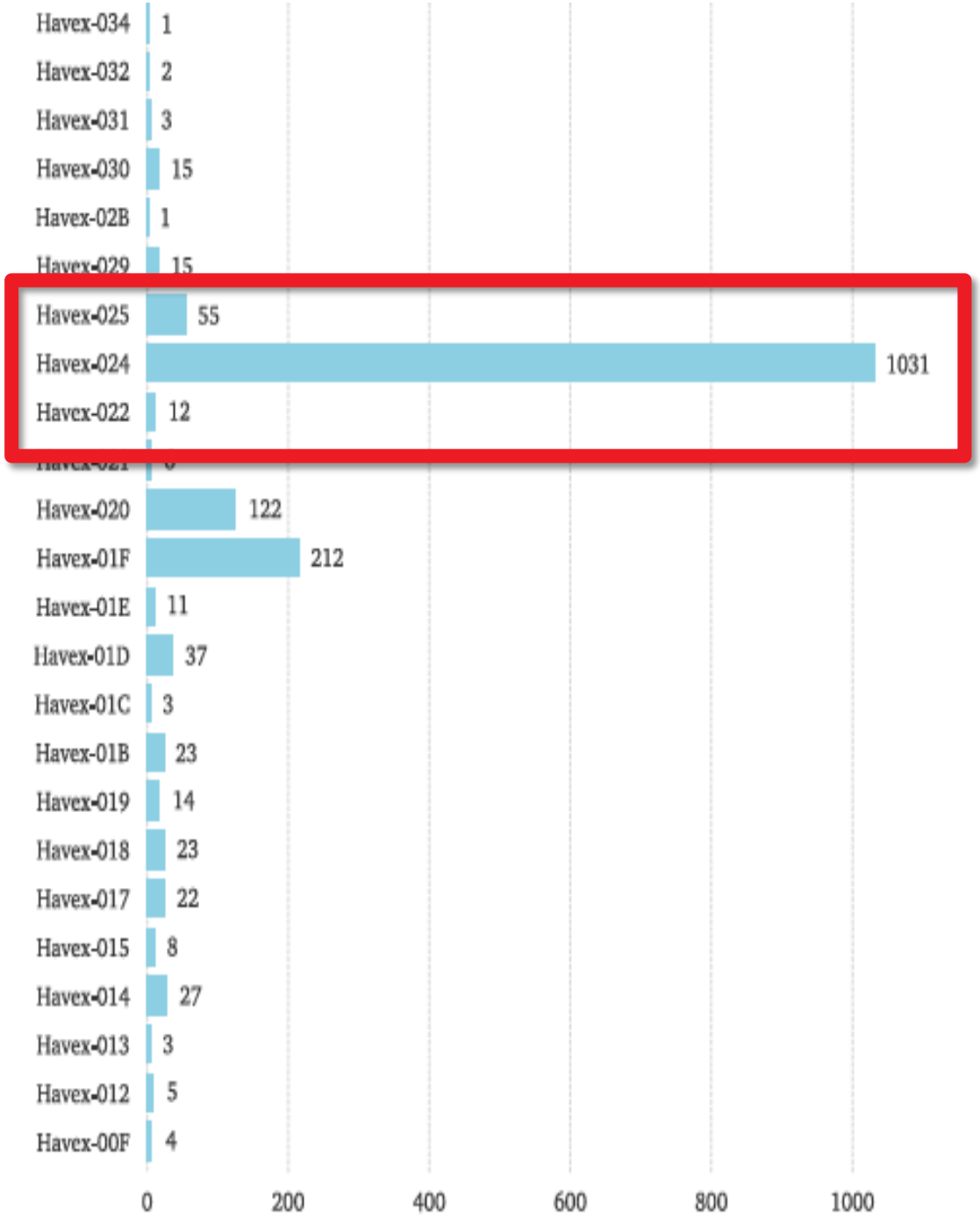
最も使われた HAVEX

- 2,470 (2,811中）台に感染したバックドア、多くが米国とスペインで確認された



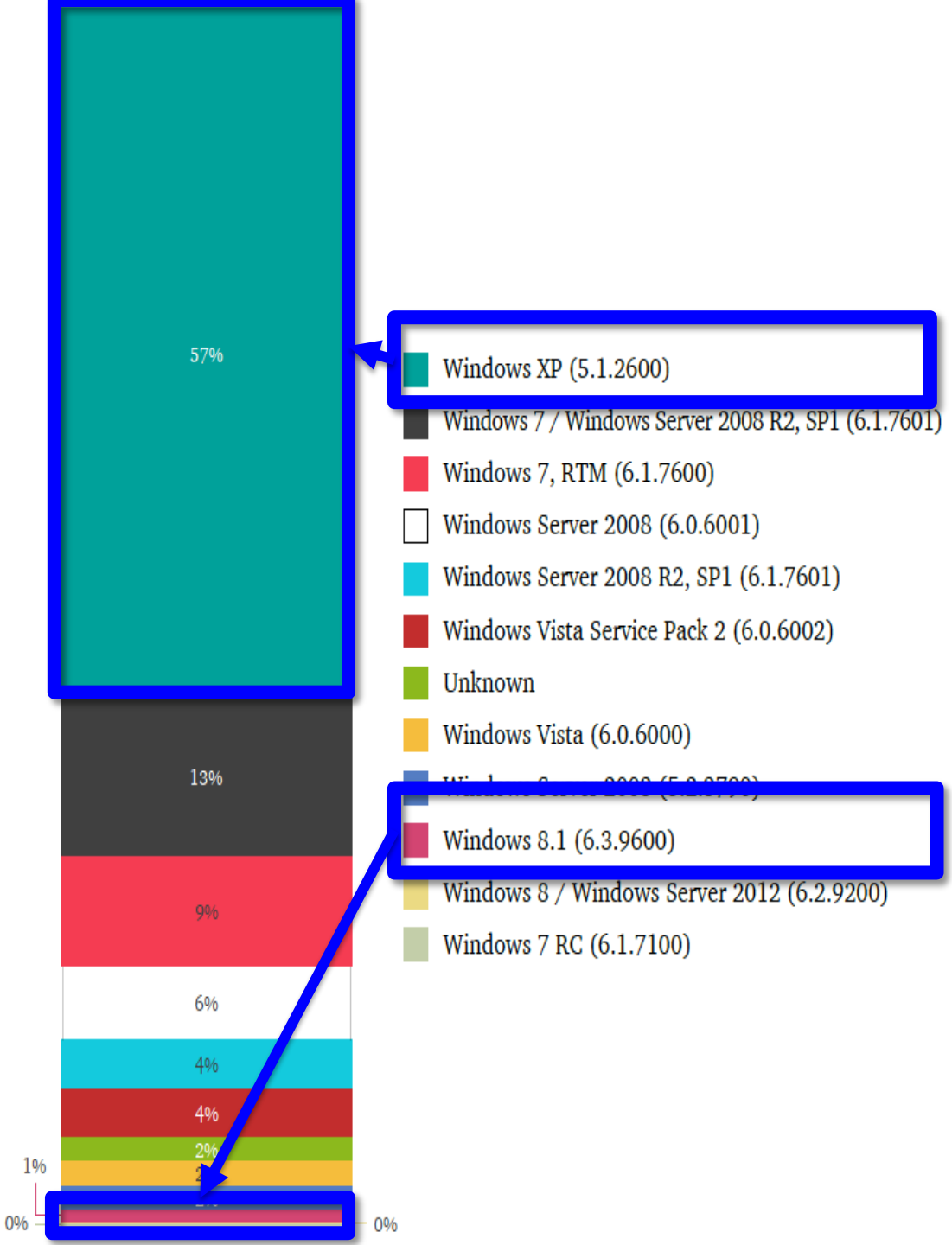
最も使われた HAVEX

- 2012年末にコンパイルされたVer.024がもっとも拡散した



最も使われた HAVEX

- 感染したOSの多くは Windows XPだったが、Windows 8.1の感染も確認された



HAVEX 進化の歴史：主な機能

- Havex によってさまざまな機能をダウンロードして追加、復号化と実行を行なう
- 攻撃ツールを *.xmd ファイルに暗号化して格納
- 各モジュールの構成情報はリソース内にbzip2とxorにより固定値「1312312」をBase64でハードコードして格納、29バイトのUID、344バイトの暗号鍵およびその他の情報を含む
- 収集したデータ（システムの情報Sysinfoモジュールで収集）は *.ylsファイルに保存、Havex DLLによってC2サーバーへ送信
- ログファイルは3DESで暗号化され、各モジュールには次の文字列が含まれている
“Copyright (c) J.S.A.Kapp 1994 - 1996.” (RSAEUROの暗号ライブラリーを使用している)

HAVEX 進化の歴史：主な機能

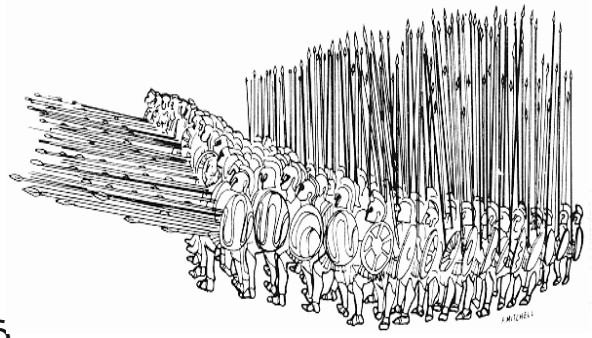
- Sysinfoモジュールで収集するHavexホスト端末のシステム情報

収集したシステム情報
Unique system ID
OS バージョン
ユーザー名
コンピューター名
国
言語
IPアドレス
ドライバーの一覧
デフォルトブラウザー
Proxy設定
ユーザー エージェント
メールの名前
BIOSバージョンと日付
デスクトップ、マイドキュメントとプログラムフォルダー および、すべてのドライブのルートディレクトリ上のファイルとフォルダーの一覧

HAVEX 進化の歴史：主な機能

- コンタクト・スティーラー・モジュール
  - Outlookの連絡先情報を収集
  - outlook.nk2 ファイルを%TEMP%¥{rand}.yls ファイルに書き出す(Outlook 2007以降が対象)
- パスワード・スティーラー・モジュール
  - ブラウザーのパスワードマネージャーが管理するログイン時のクレデンシャルをダンプ
  - BrowserPasswordDecryptor 2.0 ツール を利用
    *securityxploded.com/browser-password-decryptor.php
    *対象 ; FireFox, Google Chrome, CoolNovo, Opera Browser, Apple Safari など
- ネットワーク・スキャナー・モジュール
  - OPC/SCADAソフトウェアをスキャン、一覧は後述

HAVEX 進化の歴史：バージョンアップ



- 50を超える派生バージョンが確認されているが、そのうち作成日が確認できている01から44までの特徴は以下の通り

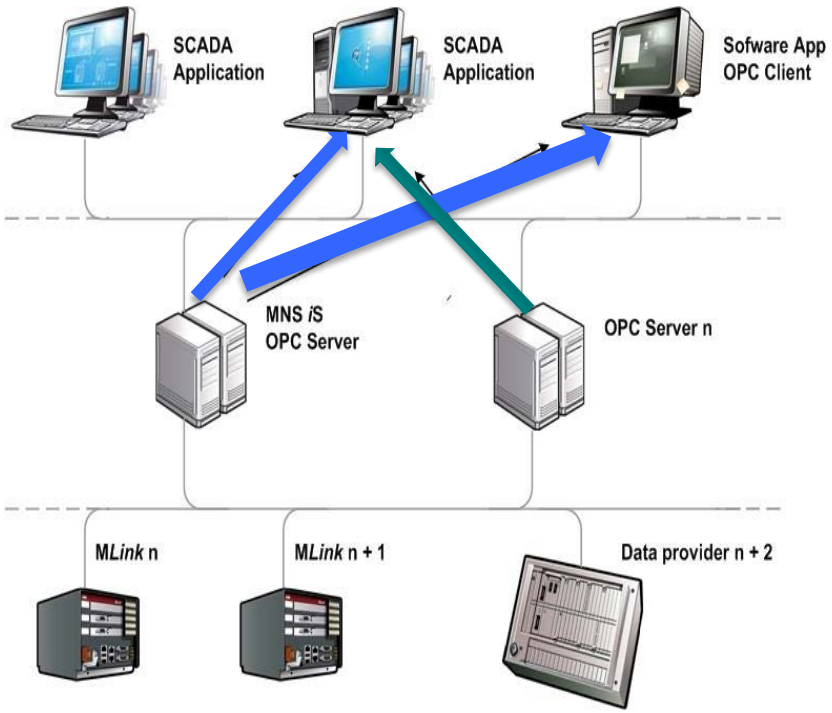
バージョン	特　徴
01-19	パスワードの収集を別途ダウンロードしたモジュールを利用して実施
17-37	GET要求を送る代わりにPOST要求をC2に送信
1A-38	レジストリからプロクシーの設定を読取り、必要に応じて利用する
1B-44	非対象暗号アルゴリズム（RSA)を使ってダウンロードしたモジュールを復号化（以前のバージョンはBase64(XOR)で暗号化）
20-25	Google.com に接続を試みてインターネット接続の有無を確認。システム情報を*.ylsファイルに書き出し。
25	“Phalanx”と呼ばれたと思われるプロジェクト用にデバッグシンボルを追加
38-40	システム情報を取り込むための*.ylsファイル処理がハードコードされた
43-44	TMPprovider0XX.dllの名前を、0xx.dllに変更

OPC って何？

- 1990年代にMcirosoft のCOM/DCOMをベースに開発が始まった、産業オートメーション分野などおける、安全で信頼できるデータ交換を目的とした、プラットフォーム非依存で、マルチベンダー間での相互運用を行うための標準規格
- 初期の規格はOPC Classicと呼ばれ、Yetiの攻撃対象となった。次世代規格であるOPC UA (Unified Architecture）がすでに存在するが、移行は進んでいない。
- OPC Foundation が保守
  - ボードメンバー(*2014) : ICONICS、Siemens AG、Honeywell Process Solutinos、Yokogawa、Rockwell Automation、Emerson Process Management

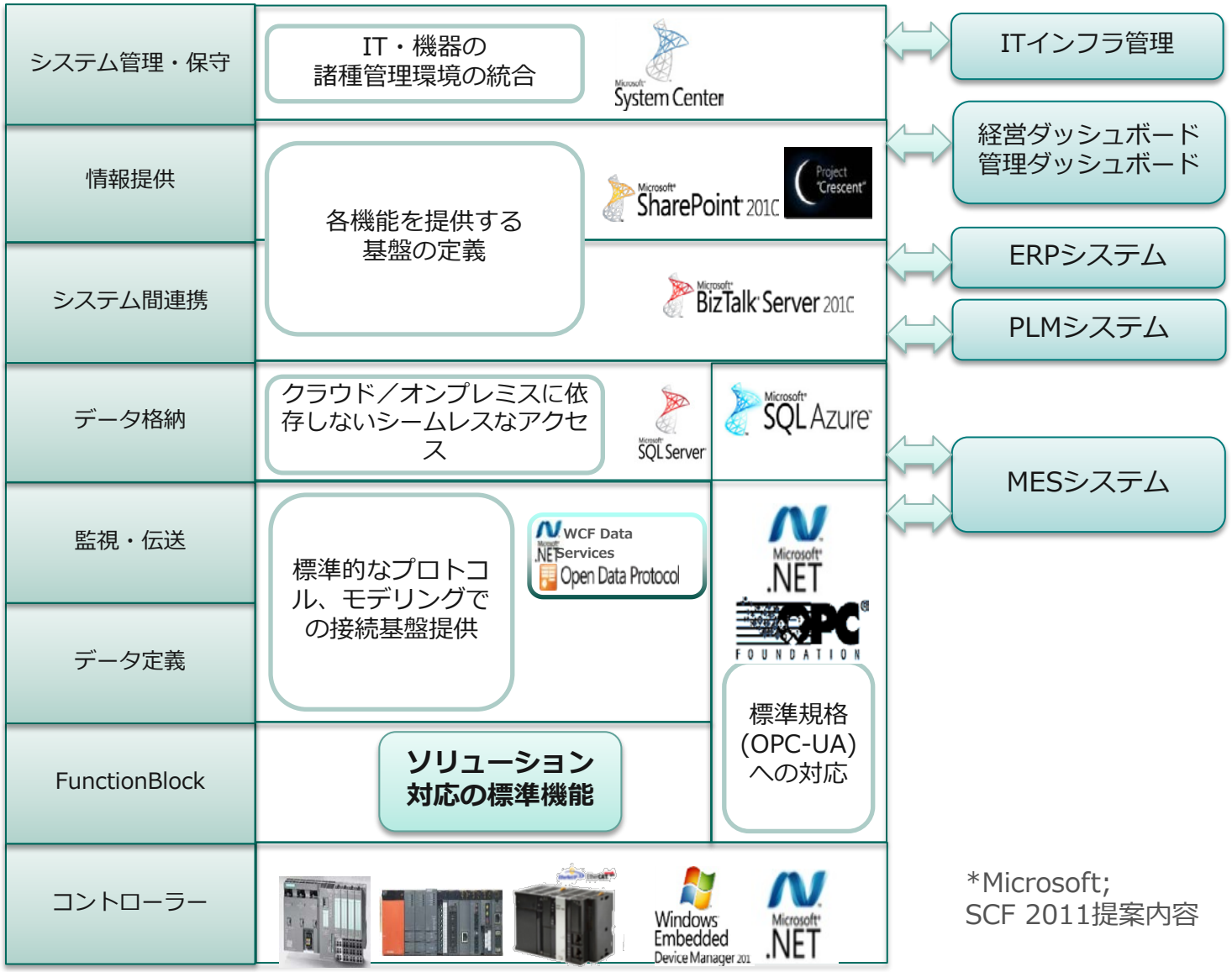
OPC のネットワーク構成例

- PLCなどの制御装置と上流のシステムとの間で利用する



*ABB;MNSiS interface manual opc server
http://www05.abb.com/global/scot/scot209.nsf/veritydisplay/294b6cf91820dfb2c1257c9b0027a55c/$file/1tgc910231m0203%20mnsis%20interface%20manual%20opc%20server%207.3.pdf

OPC のネットワーク構成例



*Microsoft;
SCF 2011提案内容

OPC CLASSIC

- 三つの仕様によって構成されている
  - OPC Data Access (OPC DA)
    値、タイムスタンプ、品質情報などのデータ交換の仕様
  - OPC Alarm & Events (OPC AE)
    状態の値と管理、同様にアラームとイベント・タイプのメッセージ交換の仕様
  - OPC Historical Data Access (OPC HDA)
    履歴データ、タイムスタンプ付きデータの問い合わせおよび分析機能のための仕様

- 主な課題
  - プラットフォーム (Windows OSとCOM/DCOM) 依存
  - セキュリティ
  - 仕様とアーキテクチャーの複雑性
  - 拡張性が低い

OPC UA(UNIFIED ARCHITECTURE)

- OPC Classicの課題を解決するため、2004年から開発が始まり、2008年に最初の実装が公開。2011年にはIEC 62541に採択。

- セキュリティのための拡張が組み込まれる
  - 監査(Auditing)
  - ユーザーアクセス制御（User Access)
  - ユーザー・アプリケーション認証(User/Application Validation)
  - 暗号化(Encryption)➔デフォルトで有効
  - 署名(Signing)➔デフォルトで有効

参照： https://jp.opcfoundation.org/resources/whitepapers/

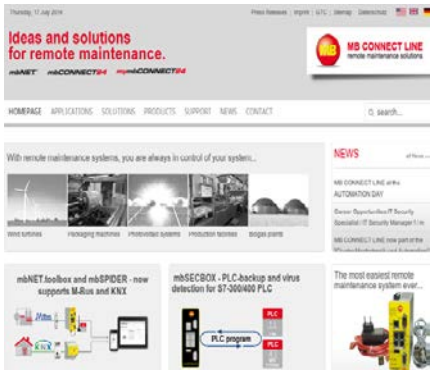
HAVEX は OPC サーバーを探し出して情報を収集

- 2014年4月11日にコンパイルされている（その後5月16日にも）
- OPC/SCADA ソフトウェア関連のポートをスキャン

ポート番号	アプリケーション
44818	Rslinx
502	Modbus
102	Siemens PLC
11234	Measuresoft ScadaPro
12401	7-Technologies IGSS SCADA

効果的な侵入シナリオ

- 正規のソフトウェアインストーラーによってマルウェアをダウンロードさせる
  - 産業用機器のデバイスドライバーや関連ソフトウェアにマルウェアのドライバーを組み込む
  - 感染したインストーラーの配布元：
    eWon（ベルギー）
    MB（ドイツ）
    Acroname（米国）



効果的な侵入シナリオ

- 悪意ある XDP ファイルによる「スピアフィッシング攻撃」
  - CVE-2011-0611 を悪用（2011年に香港の民主党のウェブサーバーでスパイウェアの感染目的で利用されていた）
    http://securelist.com/blog/incidents/30644/democratic-party-of-hong-kong-website-compromised-and-serving-spyware/

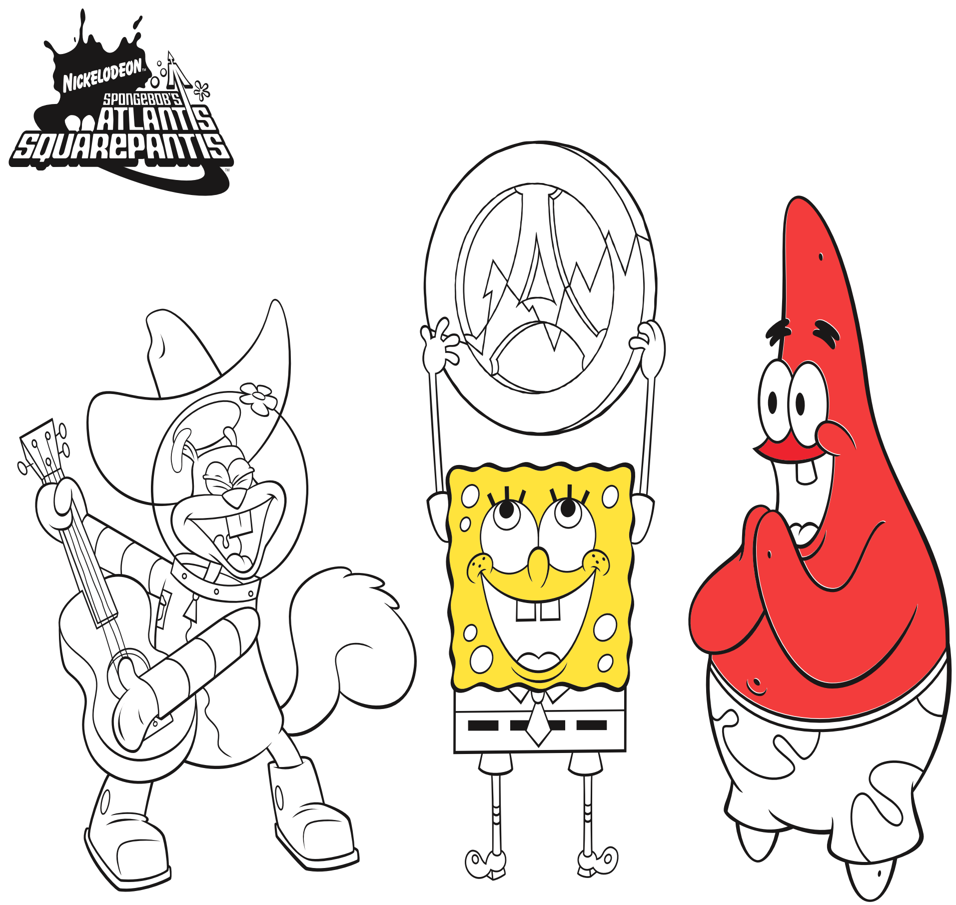
- 悪意ある JAR/Html ファイルによる「水飲み場型攻撃」
  - CVE-2013-2423 / CVE-2012-1723 / CVE-2012-4681 / CVE-2012-5076 / CVE-2013-0422 – Java エクスプロイト（多くの利用例あり）
    https://securelist.com/analysis/57888/kaspersky-lab-report-java-under-attack/
  - CVE-2010-2883 – Adobe Reader エクスプロイト（多くの利用例あり）
    http://securelist.com/analysis/monthly-malware-statistics/36327/monthly-malware-statistics-october-2010/
  - CVE-2013-2465 – IBM Java SDK エクスプロイト（NetTravelerの水飲み場攻撃で利用されていた）
    http://securelist.com/blog/incidents/57455/nettraveler-is-back-the-red-star-apt-returns-with-new-tricks/
  - CVE-2013-1488 Java エクスプロイト（Metasploitからの転用）
  - CVE-2013-1347 / CVE-2012-1889 - Internet Explorer エクスプロイト（Metasploitからの転用）
    http://old.securelist.com/en/blog/208193670/Patch_Tuesday_July_2012_Focus_on_the_Browser
  - CVE-2013-1690 – Firefox エクスプロイト（Metasploitからの転用）

効果的な侵入シナリオ：

感染サイト	特　徴
Gse.com.ge	グルジア（ジョージア）の電力システム会社
Gamyba.le.lt	リトアニア最大の電力会社
utilico.co.uk	英国のユーティリティー投資会社
yell.ge	グルジア（ジョージア）のタウンページ
chariotoilandgas.com	ナミビア、モーリタニアの石油・ガス探査会社
longreachoilandgas.com	PETROMAROC、モロッコの石油会社に買収された(2014/July)
strainstall.com	英国の測量会社
jfaerospace.com	英国の航空機製造組み立て会社（strainstall社と兄弟会社）
vitogaz.com	フランスのガス会社
bsicomputer.com	米国の産業用コンピューターシステム開発会社
energyplatform.eu	フランスの再生可能エネルギー産業プラットフォームの研究組織
firstenergy.com	カナダのエネルギー分野の投資銀行
rare.fr	フランスの環境関連の庁組織

効果的な侵入シナリオ：ちょっと違う

感染サイト	特　徴
used.samashmusic.com	米国の中古楽器販売サイト
sbmania.net	米国の「スポンジボブ」のファンサイト



まとめ

- Metasploit や既存の攻撃手法の「有効に利用」
- LightsOut エクスプロイトキットの利用は「2014年６月の期間限定」
- 業種は特定しないが特に「OPC/SCADA データを収集」
- 巧みな攻撃シナリオによる「戦略の成功」

ご清聴ありがとうございました

KASPERSKY lab