マルウェア解析の最前線と企業がとるべき対策
～脆弱性攻撃とマルウェア脅威～

Fourteenforty Research Institute, Inc.
株式会社 フォティーンフォティ技術研究所
http://www.fourteenforty.jp

ITインフラとハッカー・アンダーグラウンドの歴史

1990年代

・ハッカー・アンダーグラウンドが本格化。
・国内外で多数のハッカー・チーム結成。
・情報セキュリティの意識広がる
・情報不足であり、セキュリティ技術者もアンダーグラウンドも情報・技術をかき集めた
・セキュリティ技術者とアンダーグラウンドが同じ場所で情報交換。Full Disclosure時代。

ハッカーアンダーグラウンドの動機は「知的好奇心」や「悪戯」、「自己顕示欲」

2000年～2003年

・Web書き換え全盛、ネットワークワーム全盛
・脅威が目に見えて増加
・情報が溢れ、共有される。
・セキュリティ技術もアンダーグラウンドも急拡大。

2003年～2005年

・ 国内はWinny情報漏洩時代
・「悪戯」や「自己顕示欲」目的の攻撃は世界的に減少
・bot全盛時代
・ハッカー・アンダーグラウンドのクローズド化。ビジネスに関与

2005年～2008年

・見えない攻撃 – 標的型攻撃の本格化
・アンダーグラウンド技術の軍事目的利用の兆候
・サイバー諜報活動の本格化

そして・・・

情報セキュリティ脅威の現状

情報セキュリティを取り巻く環境は次のステージに移行。

ハッカー・アンダーグラウンドが本格化して十数年、よやく「実用段階」に。

・攻撃が見えない
・対策が難しい
・0-day利用などの高度攻撃

→ アンダーグラウンド技術が実用化されれば当然の流れ

短期的にはこの流れが加速

ハッカー・アンダーグラウンド技術の実用化

・途上国にとって「クリーン」かつ「収益性の高い」仕事
・途上国でも十分な「力」を持つことができる

一人でも優秀な技術者が居れば、既存の社会システムを使って
強大な力や財力を得ることができる。

この現象は今に始まったことではない。
表面化しなかった理由は・・・

・ 先進国の人間にその発想は無い。
  または、活用できる既存の社会システムが無い、あるいは敷居が高い。
・ 近年、途上国のIT技術が急激に成長。
  アンダーグラウンド技術が高度化。

近年の脅威の流れ

・Bot / Mass型マルウエア

無差別大量攻撃により得られた複数のマシンから構成されるBot net。
SPAM、DoS踏み台、電子商取引パスワード取得、etc…

・標的型攻撃

特定の対象を狙った攻撃。情報搾取目的に特化。
諜報活動、etc

標的型攻撃とは

特定の目標（標的）に対し、

- 経済的利益あるいは安全保障に影響を与えるなどの意図を持って、
- 情報を搾取する活動、あるいは情報搾取のための偵察活動。

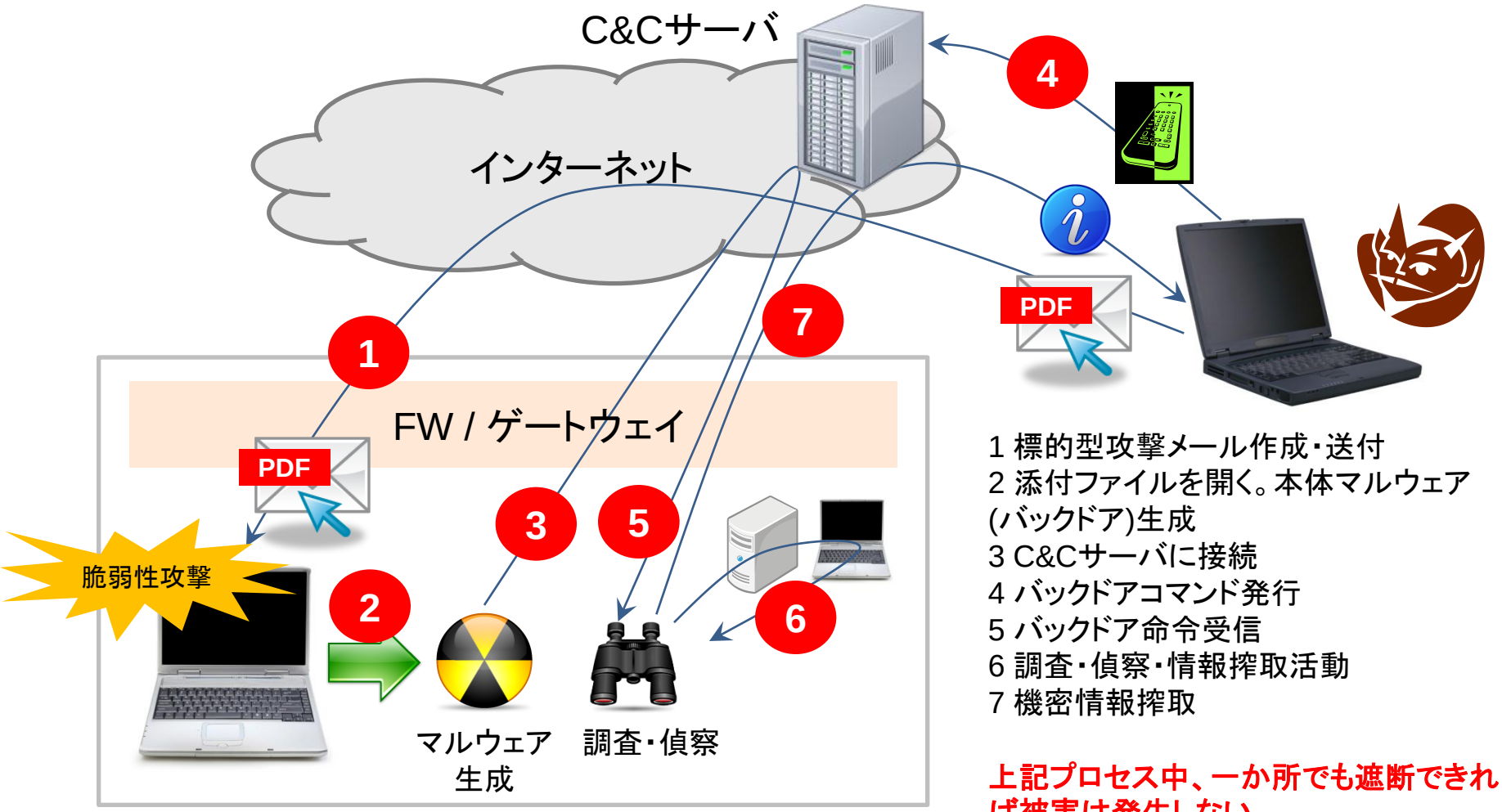
一般的には、

- ソーシャルエンジニアリングや脆弱性攻撃などのテクニックを組み合わせ、
- 標的に対してマルウェアを送信し、
- リモート制御しながら情報搾取や偵察を行う。

DDoSや大量の個人情報搾取、Web改ざん、Bot、不特定多数への未知マルウェア攻撃などが近年相次ぐが、**標的型攻撃はその背景が明確に異なる。**

標的型攻撃は、単純なウイルス攻撃ではなく、**特定の標的を狙ったハッキング**行為。
標的型攻撃に対抗するためには、**標的型攻撃に特化した戦略**を進める必要がある。

一般的な標的型攻撃のプロセス



1 標的型攻撃メール作成・送付
2 添付ファイルを開く。本体マルウェア(バックドア)生成
3 C&Cサーバに接続
4 バックドアコマンド発行
5 バックドア命令受信
6 調査・偵察・情報搾取活動
7 機密情報搾取

上記プロセス中、一か所でも遮断できれば被害は発生しない。

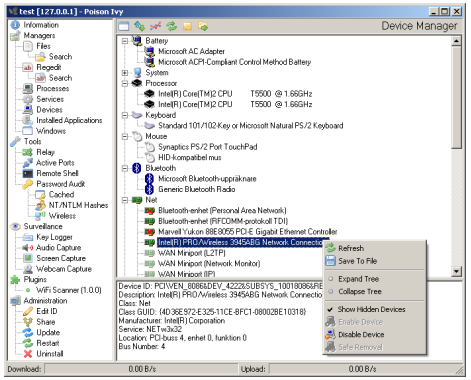
標的型攻撃における各プロセスの特徴

1. **標的型攻撃メール作成・送付**
   - 高度なソーシャルエンジニアリングによるメール文面。
   - データファイル(PDF、Office文書)による脆弱性攻撃。
   - ツール群を利用する事も。簡単に未知マルウェアを作成可能。
   - 未知セキュリティ脆弱性を利用する事も。

   ポイント1：同様の手法はBotなどでも見られるが、高度なソーシャルエンジニアリングによるメール文面は特徴的。
   ポイント2：基本的に、メールをパターン型アンチウイルスで到達前に弾く事は非常に困難。
   → 標的型攻撃検体のシグネチャは無い。
   → メールが到達し、添付ファイルが開かれる事はほぼ避けられない。

2. **添付ファイルを開く。本体マルウェア(バックドア)生成**
   - メールや添付ファイルは、本体マルウェアの単なる発射台。本体マルウェアが実際に偵察や情報搾取を実施。
   - メール、添付ファイル、本体マルウェアとも、**パターンファイルに依存したアンチウィルス技術では検知困難。**
   - **リアルタイムのパッチ適用など脆弱性攻撃対策を徹底する事は多くの組織で困難。0-dayの利用も。**

3. **C&Cサーバに接続**
4. **バックドアコマンド発行**
5. **バックドア命令受信**
6. **調査・偵察・情報搾取活動**
7. **機密情報搾取**
   - 攻撃者の指令を受信し、調査・偵察・情報搾取を行う。長期間潜伏する事も。
   - C&Cサーバは攻撃毎に変化する事が多く、**接続先をシグネチャで検知する事は困難。**
   - バックドア通信は暗号化。HTTP通信に紛れる事が多く、正常通信との区別がつきにくい。
     シグネチャベースの技術や通信ログの分析で通信を遮断する事も困難。

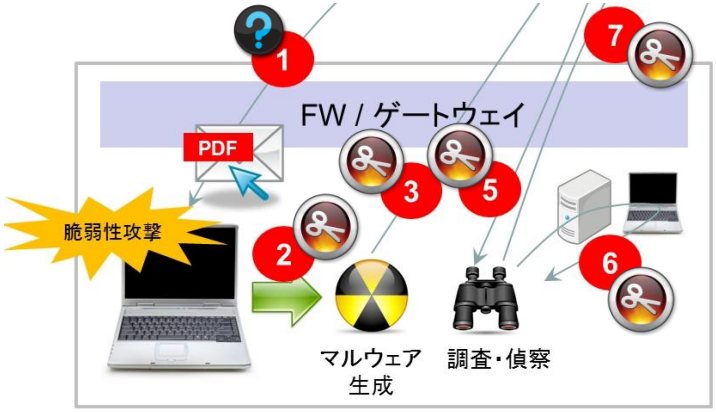


標的型攻撃と通常のウィルス対策の違い

- 標的型攻撃は「マルウェアを使ったハッキング行為」。
  マス型マルウェアなど通常のウィルス対策手法などは効果が限定的。
- マルウェアが添付されたメールが到達し、開かれる事を防ぐのはほぼ避けられない。

標的型攻撃対策のポイント:

添付されたマルウェアが開かれてから、実際に情報が流出するまでのどこかのポイントで攻撃を遮断する。多少防御でリスクを緩和。



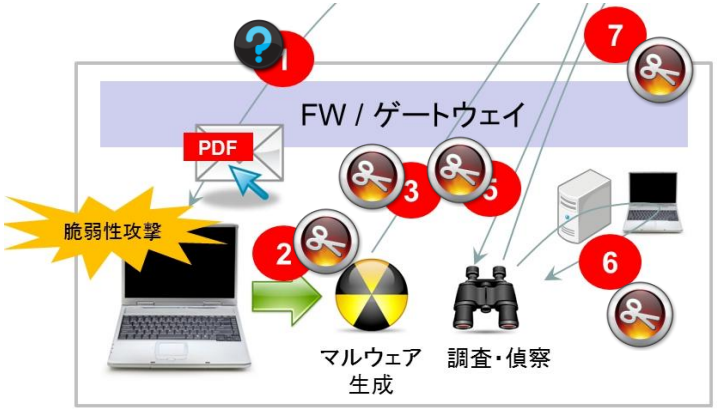
1 標的型攻撃メール作成・送付

防御ポイント
- 2 添付ファイルを開く。本体マルウェア(バックドア)生成
- 3 C&Cサーバに接続

4 バックドアコマンド発行

防御ポイント
- 5 バックドア命令受信
- 6 調査・偵察・情報搾取活動
- 7 機密情報搾取

一般的な標的型攻撃のプロセスと対抗ポイント



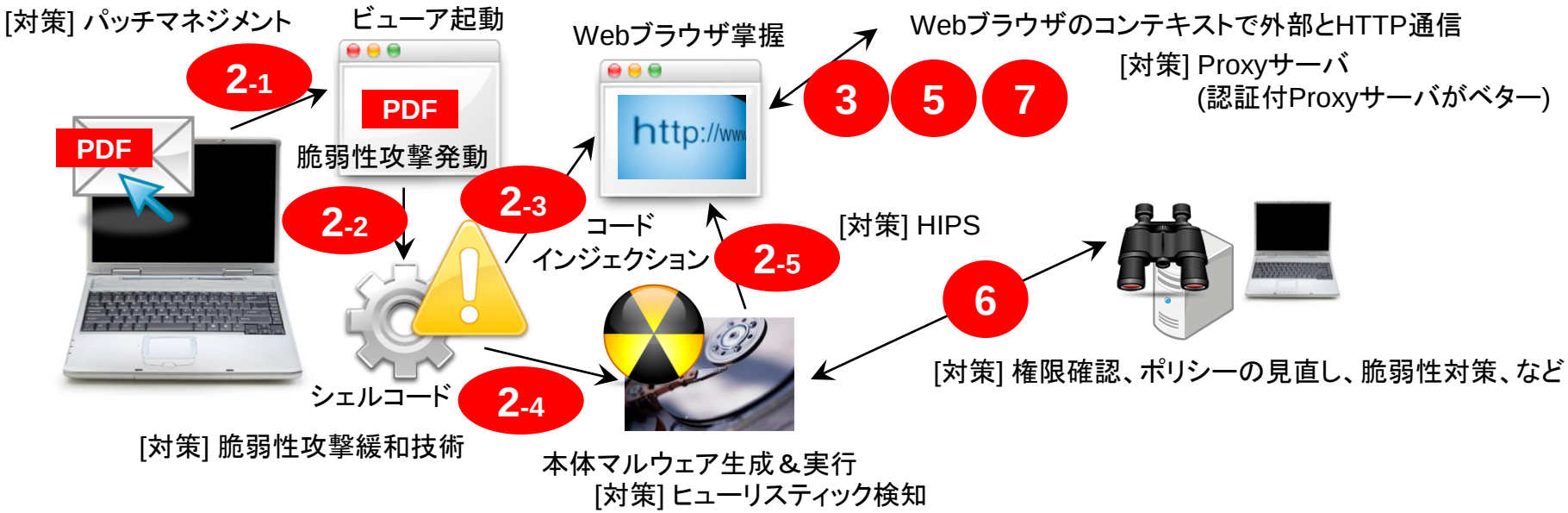
1 標的型攻撃メール作成・送付

対抗ポイント
- 2 添付ファイルを開く。本体マルウェア(バックドア)生成
- 3 C&Cサーバに接続

4 バックドアコマンド発行

- 5 バックドア命令受信
- 6 調査・偵察・情報搾取活動

対抗ポイント
- 7 機密情報搾取



三菱重工業の事例(1/3) / 報道情報ベース

- 2011年9月19日
  - 読売新聞朝刊にてサイバー攻撃を受けたとの報道
  - 夕刻、第三者による攻撃を受けていたことを関係者が発表
  - 攻撃の詳細はマルウェア感染によるもの
    - 防衛産業や原子力関係の生産・開発拠点に攻撃が集中
    - 11拠点のコンピュータ83台（PC38台/サーバ45台）が感染
  - 外部からの侵入および情報抜きとりの痕跡も見つかっている
    - 流出したのはコンピュータのシステム情報とされる（※1）
    - キーロガーにより一部サーバのパスワードが流出した可能性(※2)

※1 http://itpro.nikkeibp.co.jp/article/NEWS/20110919/368887
※2 http://www.asahi.com/national/update/1007/TKY201110070675.html

三菱重工業の事例(2/3) / 報道情報ベース

- 2009年7月ごろ
  - 標的型メールによる攻撃が開始される
- 2011年8月11日
  - 一部コンピュータへのマルウェアの感染を確認
  - 民間セキュリティ会社へ調査を依頼

2年

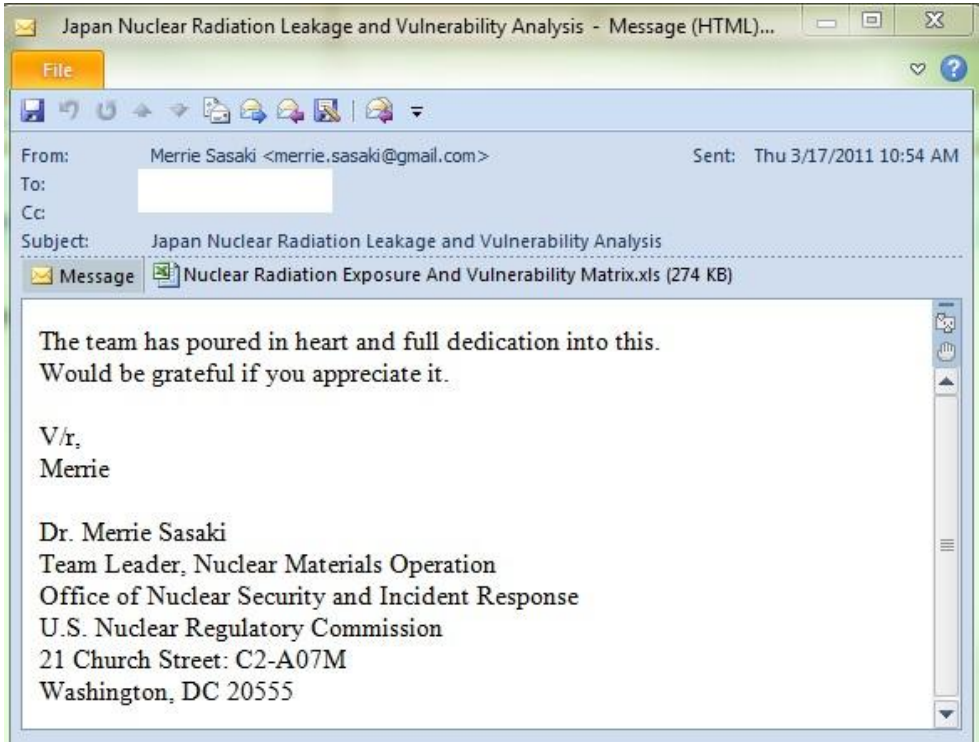
- 2011年9月19日
  - 読売新聞朝刊にてサイバー攻撃を受けたとの報道
  - 夕刻、第三者による攻撃を受けていたことを関係者が発表
  - 攻撃の詳細はマルウェア感染によるもの
    - 防衛産業や原子力関係の生産・開発拠点に攻撃が集中
    - 11拠点のコンピュータ83台（PC38台/サーバ45台）が感染
  - 外部からの侵入および情報抜きとりの痕跡も見つかっている
    - 流出したのはコンピュータのシステム情報とされる（※1）
    - キーロガーにより一部サーバのパスワードが流出した可能性(※2)

三菱重工業の事例(3/3) / 報道情報ベース

- 2011年10月25日
  - サイバー情報共有イニシアティブ(J-CSIP)が発足
    - 三菱重工、IHI、川崎重工、富士重工等の計10社が参画
    - IPAをハブとした攻撃情報の収集・共有

RSA 攻撃事例

- 2011-03-15 にcontagio blogにて確認
- Flash Exploitを含むxlsファイルが添付されたメールを確認
- 詳細不明だが、日本の原発を利用して添付ファイルを開くよう誘導した可能性がある



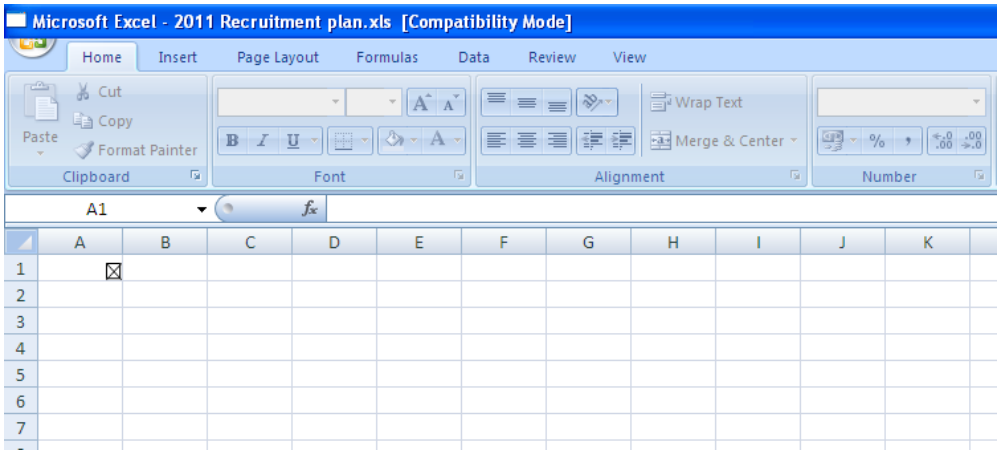
添付ファイルのハッシュ

- 4bb64c1da2f73da11f331a96d55d63e2
- 4031049fe402e8ba587583c08a25221a
- D8aefd8e3c96a56123cd5f07192b7369
- 7ca4ab177f480503653702b33366111f

CVE-2011-0609 - Adobe Flash Player ZeroDay – Update
http://contagiodump.blogspot.com/2011/03/cve-2011-0609-adobe-flash-player.html

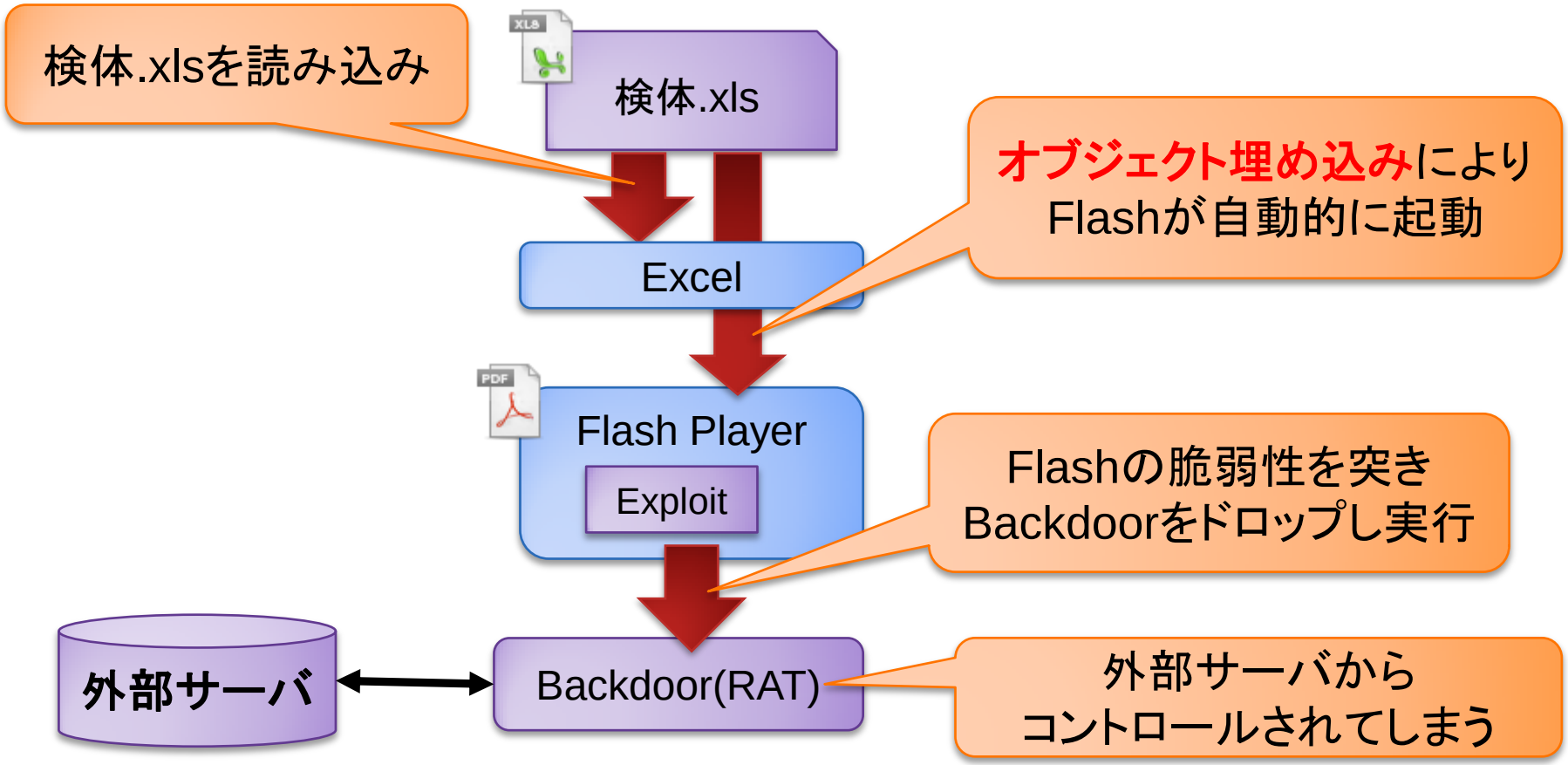
RSAの攻撃に利用されたファイル

- F-Secureの分析により以下のファイルが利用と判明
  - 1e9777dc70a8c6674342f1796f5f1c49(MSGファイル)
  - 4031049fe402e8ba587583c08a25221a(XLSファイル)
- 3月の段階でセキュリティ研究者の間で話題になっている攻撃が利用された模様



我々が「RSA」のハッキングで使用されたファイルを発見した方法
http://blog.f-secure.jp/archives/50625416.html

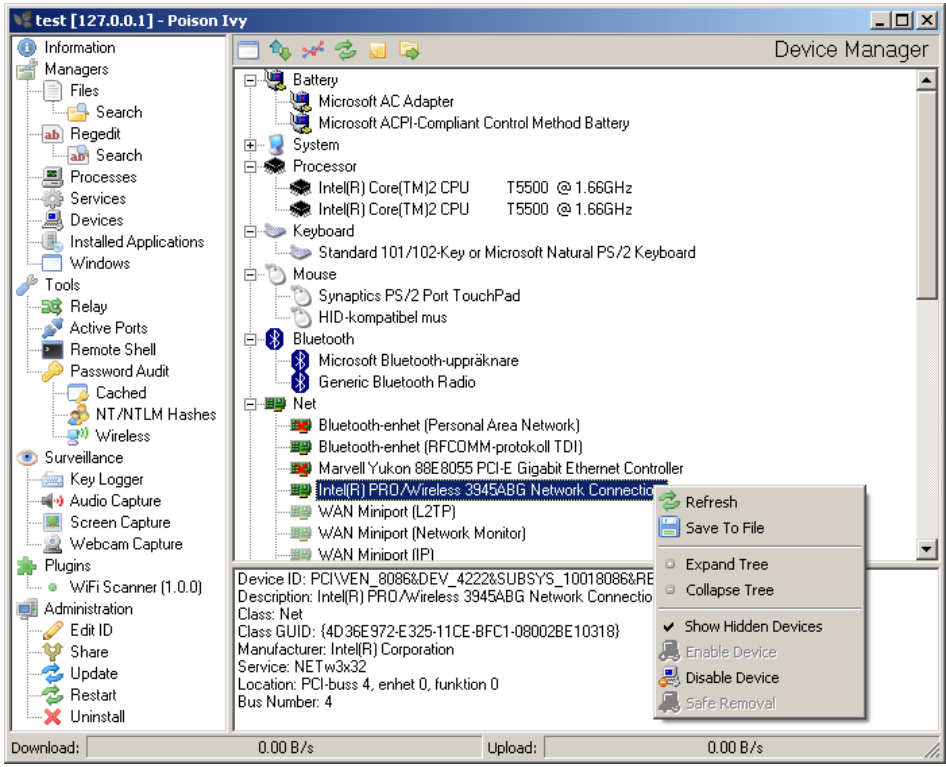
RSA標的型攻撃マルウエアの攻撃モデル



RAT(Remote Administration Tool)

- 管理者が、リモートのマシンをあたかも物理アクセスできるかのように管理する為ツール
- クライアントソフトウェアは定期的にサーバからコマンドを受信、実行する
- Firewallなどからは通常のHTTP通信に見える
- 右の図のような、商用ソフトウェア並の管理機能を持っている攻撃ツールもある

Poison Ivy – Device Manager



Poison ivy
http://www.poisonivy-rat.com/

RSA標的型攻撃マルウエアの特徴

- xls ファイルにFlashがオブジェクト埋め込みされている
  → メールの添付ファイルはxlsだがFlashが攻撃される

- RAT(Remote Administration Tool)により外部サーバからコントロールされてしまう
  - 情報収集(マシン名、OSバージョン、ユーザ名など)
  - ファイルのアップロード
  - ファイルの列挙(検索)
  - タスクの強制終了
  - コマンドの実行

  → AV機能の強制終了、機密情報の検索とアップロードなどが可能に

Duqu

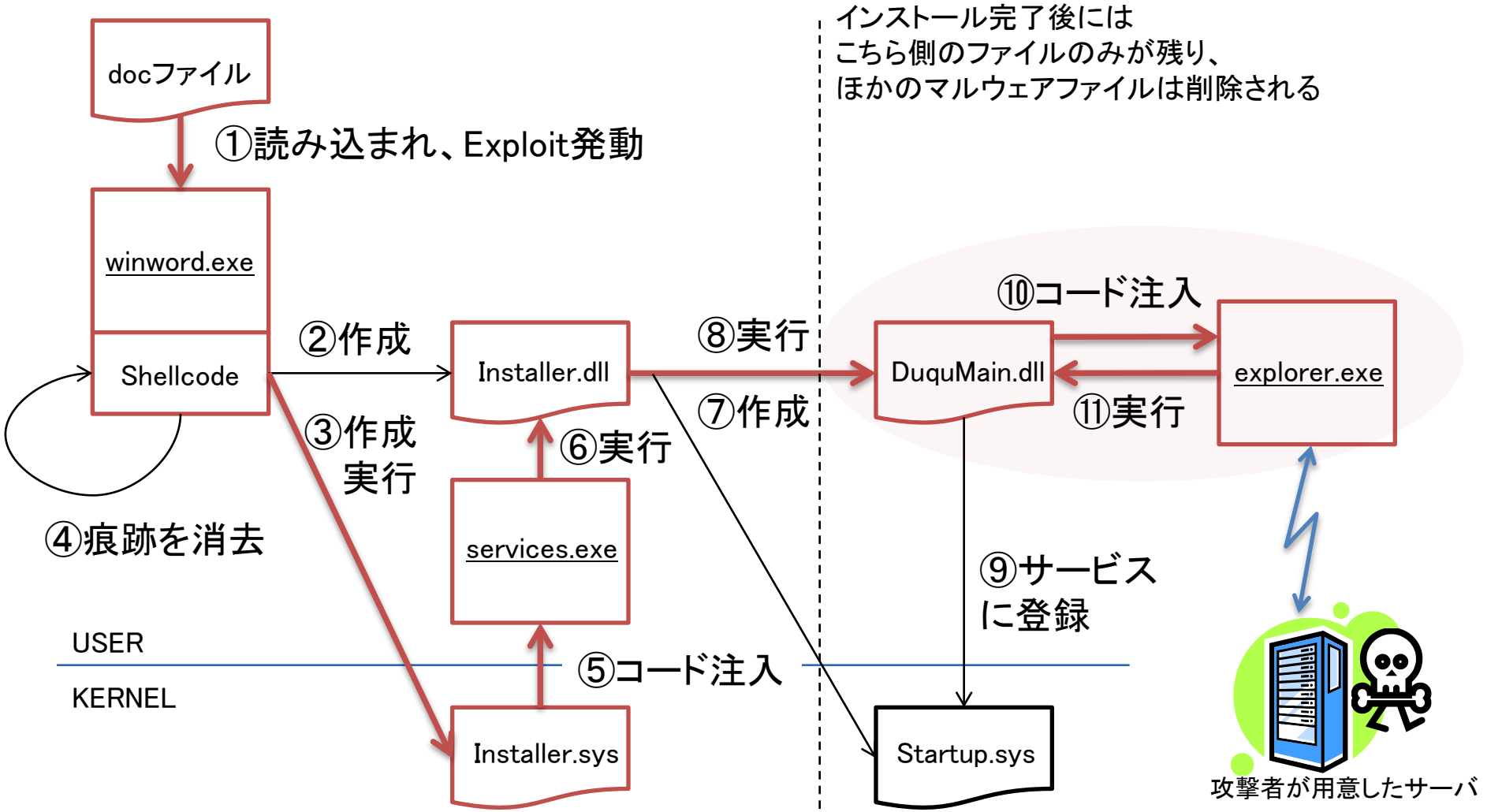
Duquとは

- 10月に報告された新種のマルウェア
- Windows カーネルの 0-day 脆弱性を用いて感染
- 感染PCの情報収集、攻撃者のサーバーに送信
- 攻撃者のサーバーから、新たなマルウェアコードをダウンロードして実行

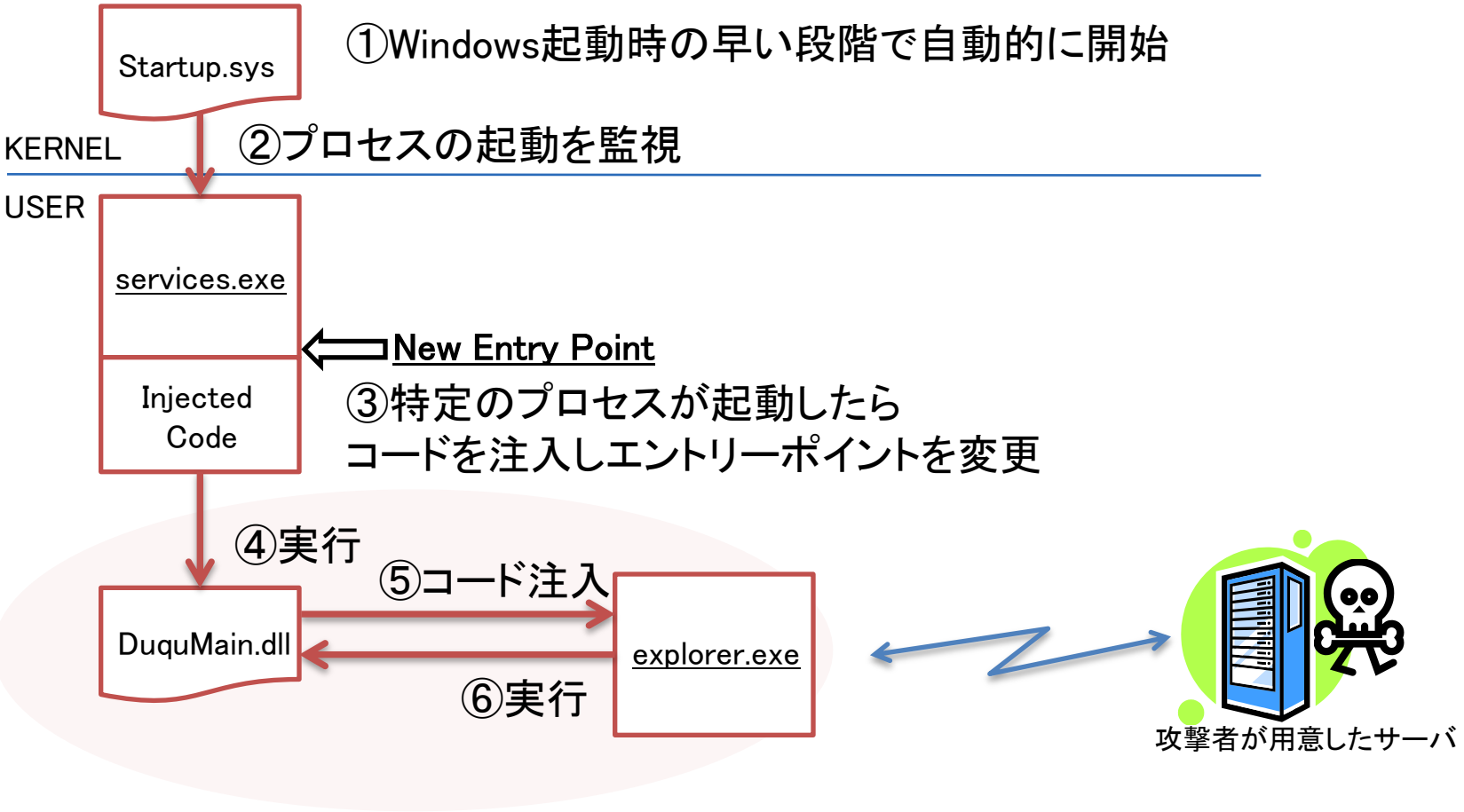
Stuxnetとの関連性

- Stuxnetのソースコードが流用されている
- 0-day 脆弱性を用いて感染する
- デバイスドライバには有効なデジタル署名が付与されている
  - 現時点では失効済み
- 標的型攻撃に用いられた

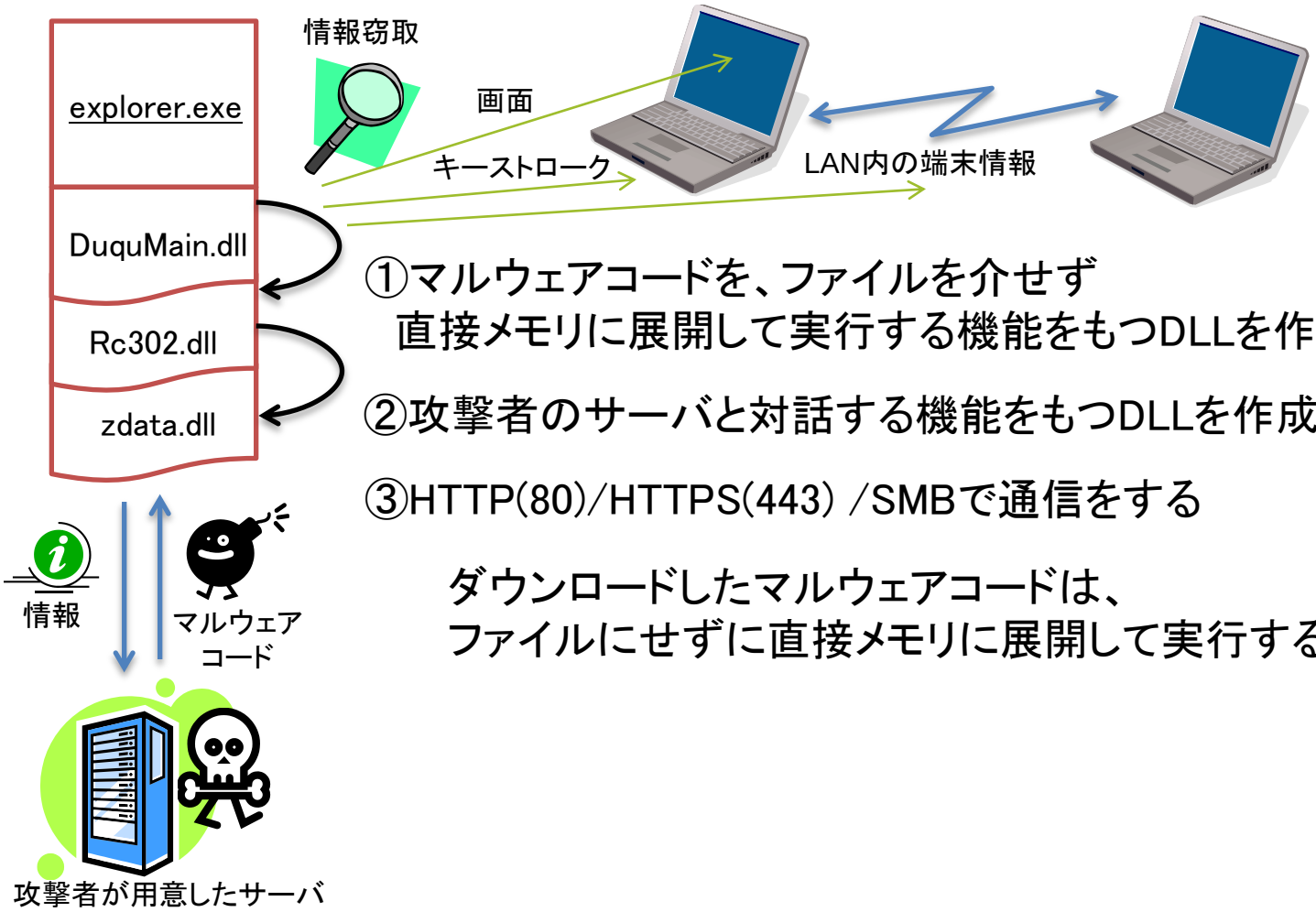
Duquの感染シーケンス



Windows再起動時の再感染シーケンス



感染後の動作



①マルウェアコードを、ファイルを介せず
直接メモリに展開して実行する機能をもつDLLを作成・読込

②攻撃者のサーバと対話する機能をもつDLLを作成・読込

③HTTP(80)/HTTPS(443) /SMBで通信をする

ダウンロードしたマルウェアコードは、
ファイルにせずに直接メモリに展開して実行する。

Duquの特徴

検出や解析を困難にする細工が多い。たとえば、

- カーネルデバッガーの検知
- 感染後、一定日数が経過すると自身を完全に削除
- マルウェアコードを、ファイルを使わずオンメモリで実行
- 多数のアンチウイルス製品に対する検出回避処理
- 攻撃者サーバーとの通信は HTTP/HTTPS を使用
  - 正常なHTTP通信の末尾に暗号化されたデータを付与して、正常な通信に見せかける

※通信内容の例

```
0000   48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d  HTTP/1.1 200 OK.
0010   0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 69  .Content-Type: i
0020   6d 61 67 65 2f 6a 70 65 67 0d 0a 4c 61 73 74 2d  mage/jpeg..Last-
0030   4d 6f 64 69 66 69 65 64 3a 20 4d 6f 6e 2c 20 31  Modified: Mon, 1
...
0000   ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01  ......JFIF......
0010   00 01 00 00 ff db 00 43 00 09 06 07 08 07 06 09  .......C........
0020   08 07 08 0a 0a 09 0b 0d 16 0f 0d 0c 0c 0d 1b 14  ................
...
1300   c3 8a 56 59 21 2f bc 41 33 b7 e2 d3 4d 75 eb 56  ..VY!/.A3...Mu.V
1310   89 73 1c 85 12 c2 a6 0c 02 51 ae f1 b1 df fe d5  .s.......Q......
1320   b1 a7 f1 9e ff 00 6b 6b cb bb 94 a0 73 1c b3 74  ......kk....s..t
1330   9a 6c d3 f1 45 dc 9f 2c a4 5e 1f 86 bc cb e8 4d  .l..E..,.^.....M
```

HTTP メッセージヘッダー(正常)

Jpegファイルデータ(正常)

Duqu独自のデータ(圧縮暗号化済)

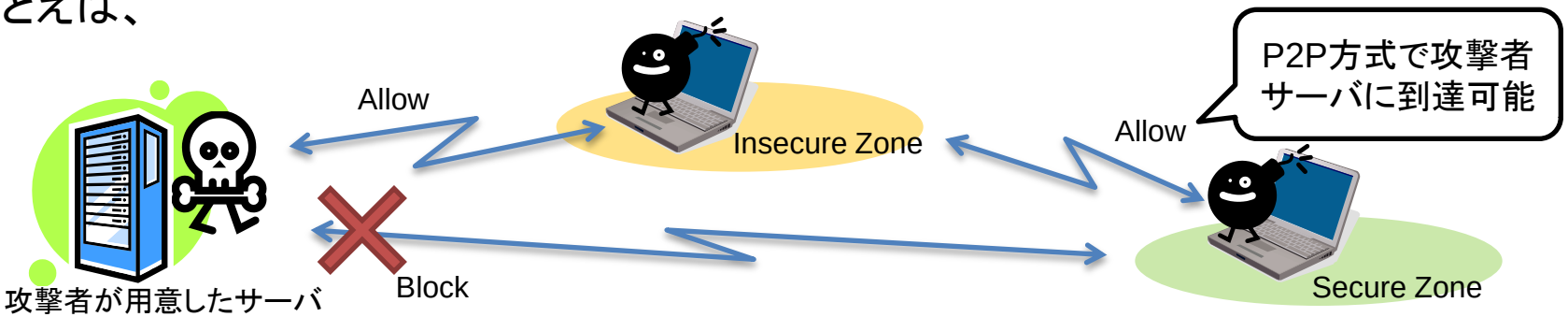
Duquの特徴

コンポーネント化されており、カスタマイズ性や状況に適用させる能力が高い。
たとえば

- C&Cサーバーと対話するためのコンポーネント(zdata.dll)
- ダウンロードしたコードを実行するためのコンポーネント(Rc302.dll)
- 情報窃取のためのコンポーネント(keylogger)

- さらに設定ファイルを与えることで動作が変更可能

攻撃者サーバーからの指示に応じて柔軟に活動可能
マルウェアの実装技術に加え、アーキテクチャがさらに洗練されてきている
たとえば、



まとめ

- **標的型攻撃への技術的対策**
  多層防御でリスクを緩和。現状を可視化し、適切な戦略立案を。場当たり的対策にならないように。
- **トレーニング**
  標的型攻撃は識別が難しいが、トレーニングを徹底すれば事故率は低下。
- **インシデント対応**
  事故前提で、緊急対応できるスキームを構築。
  アンチウイルスベンダーの情報に頼らない。
  証拠性の高い分析を行い、被害調査と適切な対策を実施する。

ご清聴ありがとうございました

Fourteenforty Research Institute, Inc.
株式会社 フォティーンフォティ技術研究所
http://www.fourteenforty.jp