macnica networks

標的型攻撃対策
世界に通じるセキュリティ

# 攻撃者を知るためのインテリジェンスの活用
## ～ 入口、出口、そして侵入拡大へ ～

マクニカネットワークス株式会社
セキュリティ研究センター
政本 憲蔵



## 最近日本を攻撃している攻撃者

### Aurora Panda

- Operation Aurora（2010年1月）の実行グループ。
- Bit9社を攻撃しコードサイニング証明書を盗む。（2013年2月）
- 米国、ドイツ、イタリア、日本など、ターゲットは広範囲に渡る。
- 製造業、メディア、防衛産業などを狙い攻撃。
- スキルが高い。

### Dagger Panda

- 少なくとも2011年3月から日本、韓国をターゲットに活動していることを確認。
- 狙われている産業は、メディア、重工業、造船と多岐にわたる。
- CVE-2012-0158の脆弱性を利用。（Officeの脆弱性）
- 以前に使ったC2サーバ名（icefog.8.100911.com）から、カスペルスキー社ではicefogと呼んでいる。C2サーバ上のアプリケーションが「尖刀三号（Dagger Three）」という名称。
- C2のプロトコルとして、HTTP(S)だけでなく、メール系プロトコルなども使う。

## Kill Chain

- **いずれかのステップでチェーンを断ち切る。（多層防御）**

| | |
|---|---|
| 偵察 | 企業サイト、SNSなどのオープンな情報からターゲットの情報（組織、取引先など）を収集。マルウェア配布やC2で使えそうな正規サーバを探すことも。 |
| 武器化 | 攻撃コード（エクスプロイト）とマルウェア（実行ファイル）の作成。 |
| 配送 | 取引先などになりすましたメール（攻撃コード/マルウェアを添付）を送付。またはマルウェアを事前に仕込んだWebサイトへアクセスさせ、ドライブバイダウンロード。 |
| 攻撃 | ユーザに添付ファイル（PDF、Office）を開かせる、もしくは悪性Webサイトへアクセスさせ、脆弱性を利用した攻撃コード（エクスプロイト）を実行する。 |
| インストール | 攻撃コードの実行された結果としてマルウェア（実行ファイル）がインストールされる。もしくはメールに添付した実行ファイルを開かせることでインストール。 |
| 遠隔操作（C2） | C&Cサーバへ接続させ、端末を遠隔操作する。必要に応じて、追加のマルウェアやツールをダウンロードする。 |
| 侵入拡大 | 管理者権限への昇格後、ディスク・メモリに保存されたパスワード・ハッシュを抜き出し、Pass-the-Hash攻撃で他のコンピュータに足掛かりを作りながら、ネットワークを動き回る。 |
| 目的実行 | 目的の情報を探し、暗号化および細分化してから外部へ持ち出す。 |

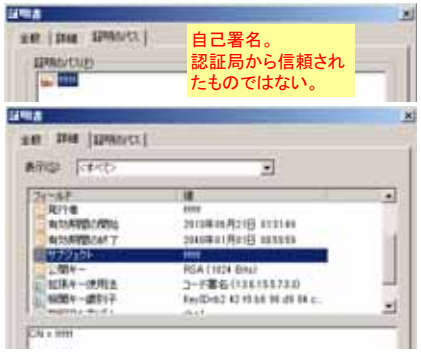
## 犯罪者向けAVスキャンサービス

- http://www.virtest.com/
- http://chk4me.com/
- http://scan4you.net/

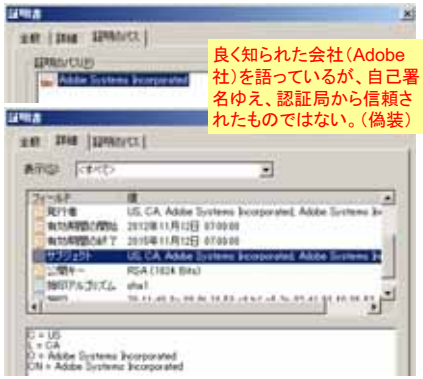
# デジタル署名が付いたマルウェア　レベル1

Win.Trojan.ZeroAccess
MD5 Hash: 6be3f62831007247156f65cf12b9665f



自己署名。
認証局から信頼されたものではない。

Win.Trojan.Dokstormac
MD5 Hash: 9576c9d64a8eaefb1c76e099cba98813



良く知られた会社（Adobe社）を語っているが、自己署名ゆえ、認証局から信頼されたものではない。（偽装）

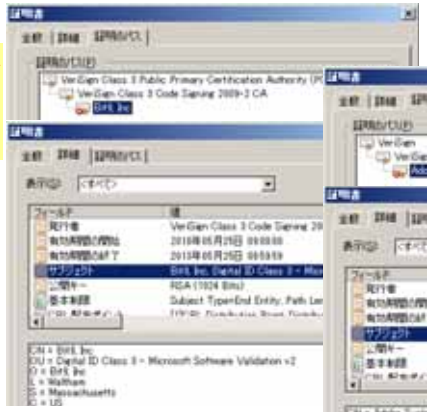



# デジタル署名が付いたマルウェア　レベル10

- Adobe
- Opera
- Bit9

上記の会社を攻撃し、盗んだコードサイニング証明書を使って、マルウェアにデジタル署名を追加。

Aurora Pandaのドロッパー
MD5 Hash: 918f76b341b40af346ae7a1358548799



Deep PandaのRAT
MD5 Hash: 46db73375f05f09ac78ec3d940f3e61a

**Bit9社がAurora Pandaに攻撃を受けた際の調査結果：**
**https://blog.bit9.com/2013/02/25/bit9-security-incident-update/**




# デジタル署名が付いたマルウェア　レベル5

McAfee社によると、6.6%のマルウェアに正規のデジタル署名が付いている。

McAfee research shows sharp rise in malware signed with legitimate digital certificates

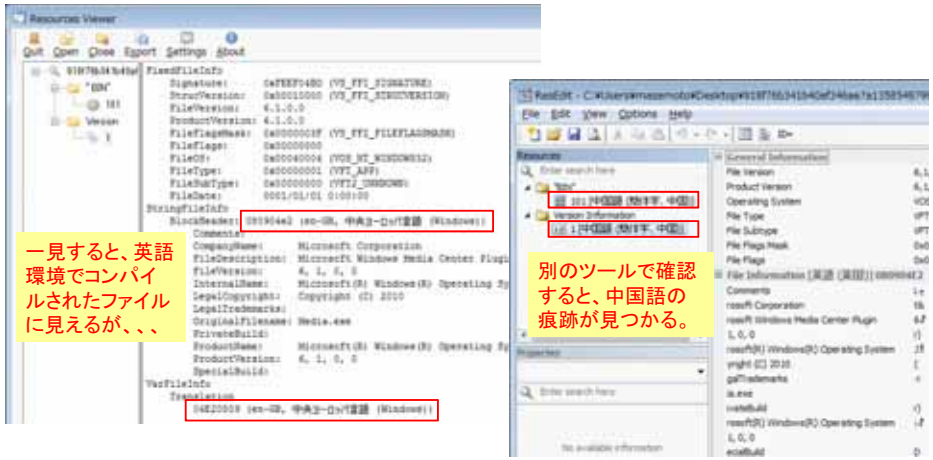
デジタル署名は、偽造や盗んだものではない。認証局から正規に発行されたコードサイニング証明書によって追加されたデジタル署名ものである。

**http://www.networkworld.com/news/2013/100313-mcafee-malware-274481.html**




# 言語を偽装

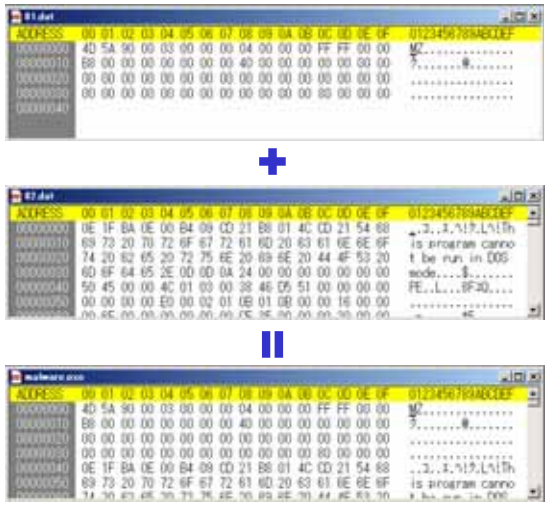
- Aurora Pandaのドロッパー（MD5 Hash: 918f76b341b40af346ae7a1358548799）のリソース



一見すると、英語環境でコンパイルされたファイルに見えるが、、、

別のツールで確認すると、中国語の痕跡が見つかる。

## マルウェアの分割



マルウェアを分割して配送することで、途中経路にあるセキュリティ製品の検知を回避。

結合するためのロジックは、別のマルウェア検体に含まれているケースが多い。



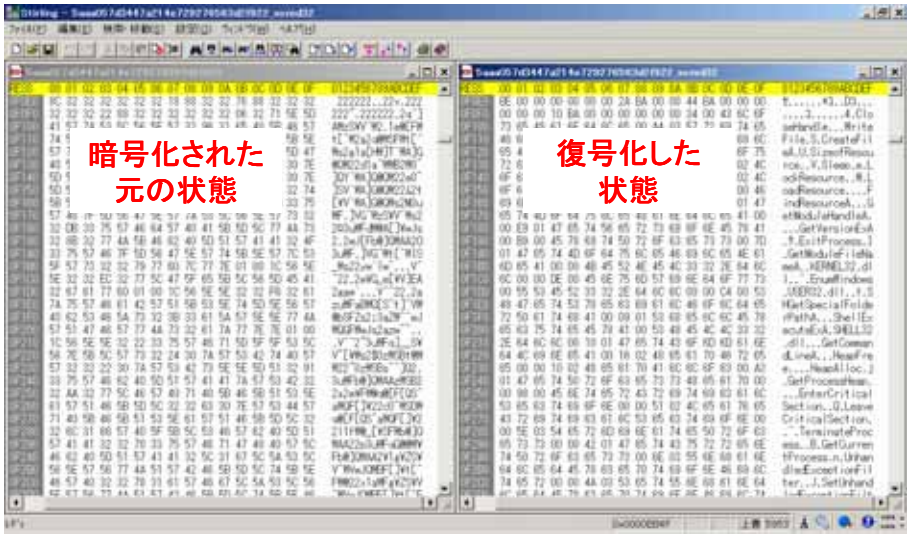

## 代替データストリーム（ADS）

- **NTFSファイルシステムにおいてサポートされた標準機能**
  - 作成者、タイトル、サムネイル画像といったファイルの属性情報が格納される。
  - Windows上のエクスプローラからはその存在が表示されない。
  - Vista以降では、dirコマンドのオプション（/r）で確認できる。
- **マルウェアの隠し場所として利用されたことがあった。**
  - 一昔前は、アンチウイルス製品で検知できなかった。
  - 現在でも、攻撃者は、アンチフォレンジックの目的で隠し場所として利用することがある。

```
c:¥temp>type malware.exe > hoge.txt:malware.exe
c:¥temp>mklink backdoor.exe hoge.txt:malware.exe
c:¥temp>backdoor
```



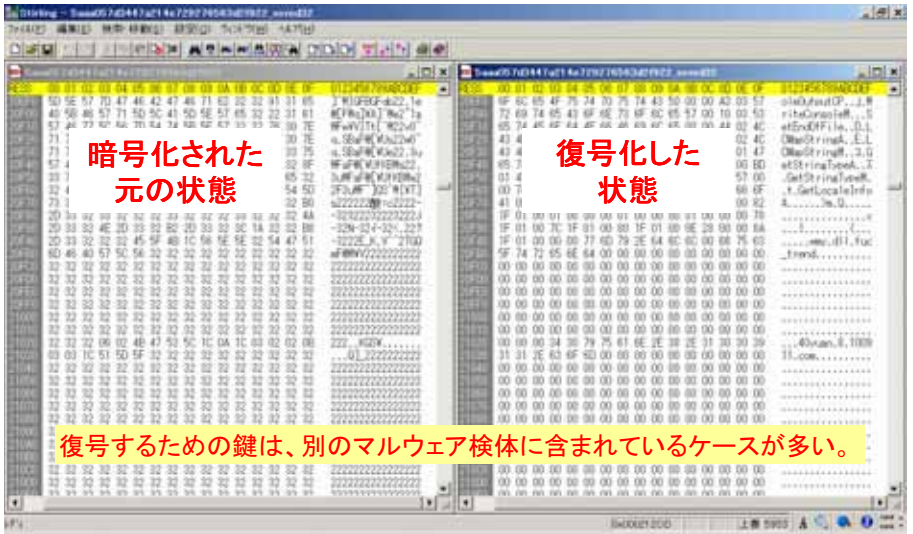

## XOR暗号されたマルウェア



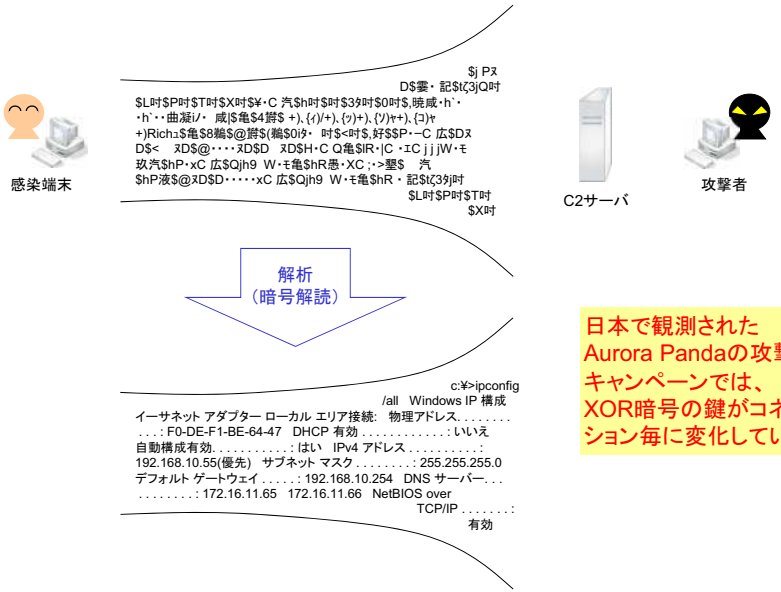




## XOR暗号されたマルウェア



## XOR暗号されたC2通信




日本で観測された
Aurora Pandaの攻撃
キャンペーンでは、
XOR暗号の鍵がコネク
ション毎に変化していた。




## 正規通信に偽装するC2通信

- 独自プロトコルから一般プロトコルへ
  - HTTP(S)
  - DNS （TXTレコード）
  - ICMP
- 正規サーバと通信
  - Google翻訳を経由してC2サーバと通信
  - Twitterのツブヤキをコマンド
  - 脆弱性をかかえた正規サイトをハッキングしてC2サーバに仕立てる
  - ClouDNS




## マルウェアによる情報収集

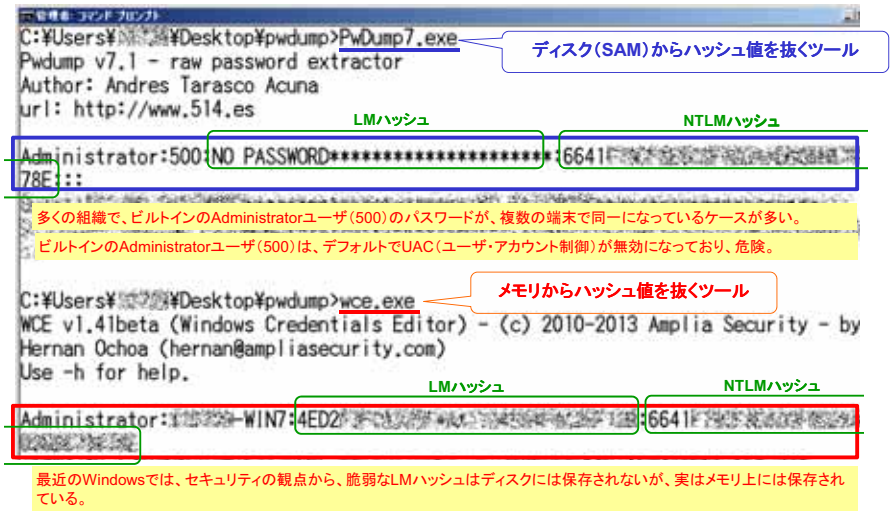
```
c:¥>ipconfig /all
c:¥>netstat -an
c:¥>netstat -rn

c:¥>net view /domain:masamoto
サーバー名            注釈
-------------------------------------------------------------------------------
¥¥NEWB-PC
¥¥WIN-TSQ
¥¥HQADMIN
¥¥ADMIN123
コマンドは正常に終了しました。

c:¥>net use
新しい接続は記憶されません。

ステータス       ローカル名       リモート名                    ネットワーク名
-------------------------------------------------------------------------------
OK               N:               ¥¥fileserv¥HQ                 Microsoft Windows Network
切断                              ¥¥192.168.128.180¥IPC$        Microsoft Windows Network
コマンドは正常に終了しました。

c:¥>find /n /i "secret" c:¥Users¥Administrator¥Documents¥*.*
```

感染端末上で、マルウェアは
様々な情報を収集し、組織内の
ネットワークを把握していきます。

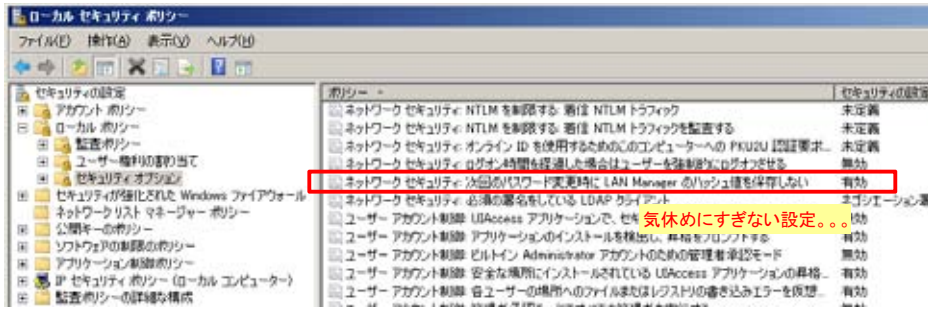
IPアドレス
通信している内部サーバ
ルーティング情報
ファイルサーバ
機密ファイルの場所
など。。。




## パスワードを窃盗するアプローチ（LM/NTLMパスワード・ハッシュ）



## パスワードを窃盗するアプローチ（LM/NTLMパスワード・ハッシュ）




- たしかにハードディスク（SAM）には保存されないが、メモリ上にはLMハッシュ値が保存される。
- LMハッシュは脆弱で、解析しやすい。
  - 14文字までのパスワード。（15文字以上はNTLM）
  - 大小文字区別なしで全て大文字に変換される。
  - アルゴリズムが脆弱。
  - パスワード総数は約7兆5000億と少なめ。




## パスワードを窃盗するアプローチ（LM/NTLMパスワード・ハッシュ）

LM/NTLMハッシュの取得した後は、

- レインボーテーブルでパスワードを解析。（Pass-the-Pass攻撃）

もしくは

- **Pass-the-Hash**攻撃で他の端末へ侵入。
  - パスワード・ハッシュ値だけでログイン可能。（パスワードそのものは不要）
  - ファイル共有プロトコル（SMB）を使って、リモートからコマンドを実行。
  - PsExecなどの正規のリモート管理ツールを使うことが多い。
    - http://technet.microsoft.com/ja-jp/sysinternals/bb897553.aspx
  - 脆弱性は不要。
  - マイクロソフト社はPass-the-Hash攻撃に対する修正はリリースしない（できない）。
    - http://www.microsoft.com/en-us/download/confirmation.aspx?id=36036




## パスワードを窃盗するアプローチ（LM/NTLMパスワード・ハッシュ）

- 攻撃者は、ドメイン管理者などの高い権限ユーザを持ったユーザのパスワード・ハッシュを狙っている。
  - PCに潜むマルウェアが故意に問題を起こして、管理者によるログインを誘惑し、管理者のハッシュ値を盗む。
  - 管理者のRDPなどによるリモート・メンテナンスにより、従業員PCのハードディスク・メモリに管理者のハッシュ値が残存してしまう。

管理者によるリモート・メンテナンスなどに、ドメイン管理者などの高い権限のユーザを使うのは非常に危険。



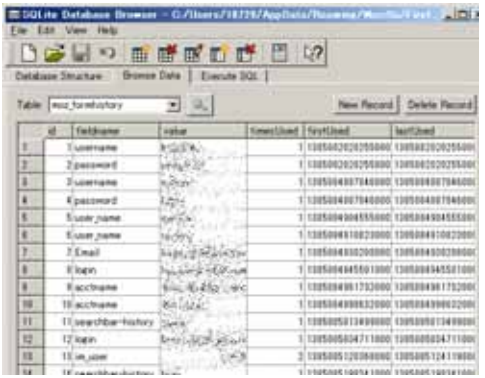

## パスワードを窃盗するアプローチ（その他）

- **ブラウザのフォーム履歴**
  - IE

    C:¥Users¥<username>¥AppData¥Local¥Microsoft¥Internet Explorer¥Recovery¥High¥Last Active¥*****.dat
  - Firefox

    C:¥Users¥<username>¥AppData¥Roaming¥Mozilla¥Firefox¥Profiles¥*****.default¥formhistory.sqlite
- **ARPスプーフィング ＋ Sniffing**
- **キーロガー**

Firefoxのフォーム履歴ファイル（formhistory.sqlite）をSQLiteブラウザで閲覧したところ



## パスワードを窃盗するアプローチ（その他）

- Chromeの場合





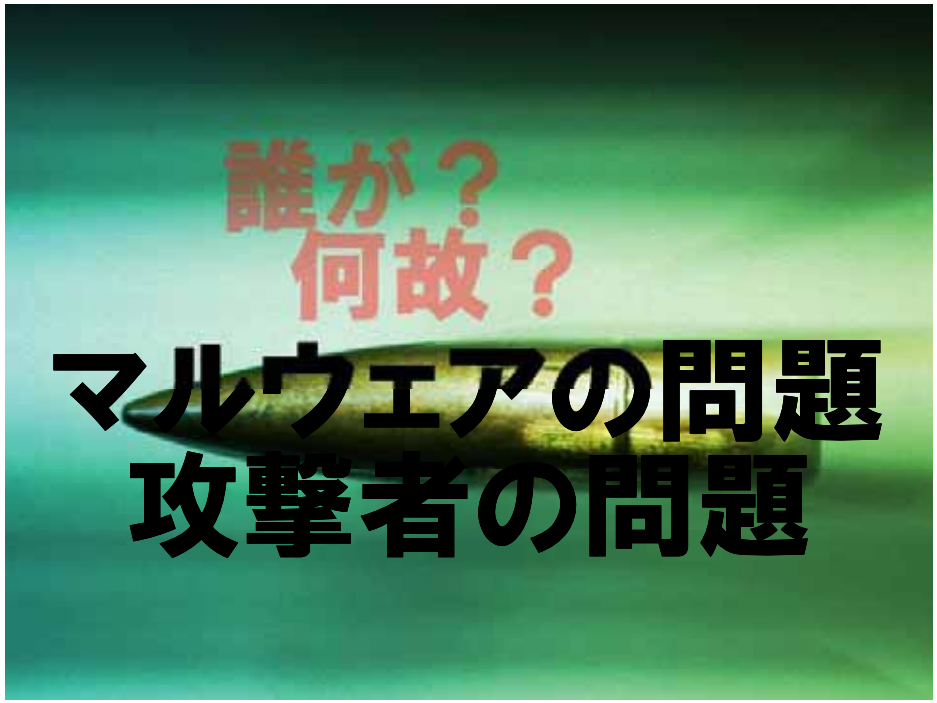
## ソリューション・マトリックス

| | 既知の脅威に対する対策（≒ バラマキ型攻撃対策） | 未知の脅威に対する対策（≒ 標的型攻撃対策） |
|---|---|---|
| 偵察 | Firewall | |
| 武器化 | IPS | |
| 配送 | Spam Firewall / URL Filter | |
| 攻撃 | パッチ管理 | |
| インストール | AV | |
| 遠隔制御（C2） | IPS / URL Filter | |
| 侵入拡大 | ー | |
| 目的実行 | DLP | |

CROWDSTRIKE
FireEye
BLUE COAT
McAfee An Intel Company
Infoblox

標的型攻撃対策は、既知の脅威対策とは別に設計・実装する必要がある。




## 攻撃者のROI

知的財産の価値 ＞攻撃にかかるコスト

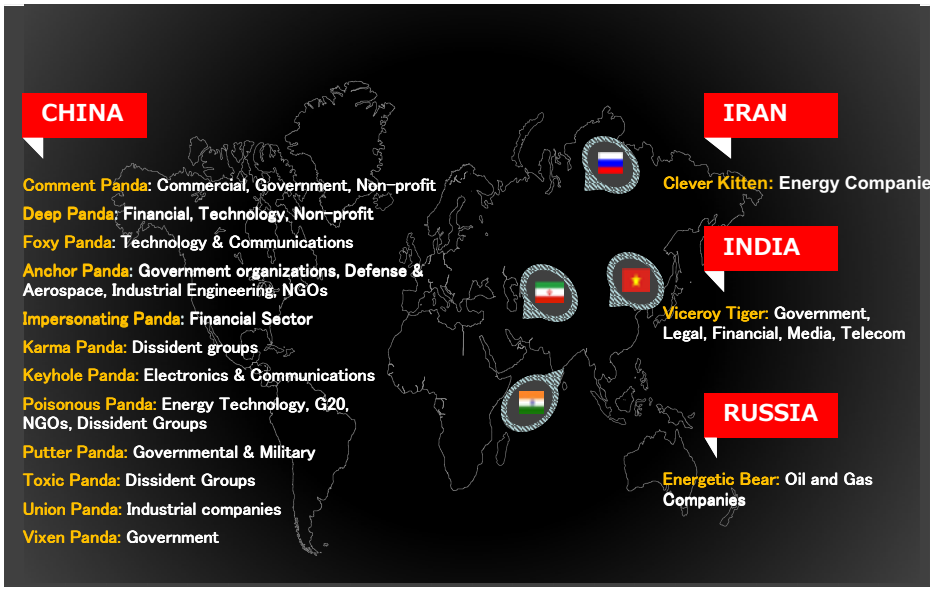
攻撃します

## CrowdStrike(クラウドストライク)会社概要

- 本社:アメリカ(カリフォルニア州アーバイン)
- 事業:大企業や政府機関における知的財産や国家機密情報の保護
- セキュリティのドリームチーム
  - George Kurtz(ジョージ・カーツ), President/CEO & Co-Founder
    - 元McAfee社のCTO(Foundstone社の創設メンバー)
    - セキュリティのベストセラー「Hacking Exposed」の著者の一人
  - Dmitri Alperovitch(ドミトリ・アルペロヴィッチ), CTO & Co-founder
    - 元McAfee VP of Threat Research
    - 「Operation Aurora」「Night Dragon」「Shady RAT」解析者で名付け親
  - Shawn Henry(ショーン・ヘンリー), President CrowdStrike Services
    - 元FBIのサイバー犯罪部門の責任者




## Adversary Groups







## Intelligence Report

- マルウェア検体やC2をリバースエンジニアリングした調査結果を元に、攻撃者に特有のTTPs(Tactics, Techniques, and Procedures)に関する情報が満載。
  - マルウェア・バイナリの暗号化手法
  - C2の暗号化手法
  - C2の暗号化データを復号化するためのスクリプト(Python)
  - C2の通信内容、実装コマンド
  - 攻撃の痕跡(ファイルシステム、レジストリ、ハッシュ、カーネルドライバ)
  - 感染後に使用するツールや役割
  - 攻撃者の人物的な個人情報、背景
  - etc.




## サンプルレポート

- サンプルレポートをご覧になりたい方は、

CrowdStrike Deep Panda 検索

## Actionable Intelligence Feed

偵察
武器化
配送
攻撃
インストール
遠隔操作（C2）
侵入拡大
目的実行

- Yaraルール
- Snortルール
- CSVデータ
  - IPアドレス、ドメイン、URL
  - ハッシュ（MD5、SHA1、SHA256）
  - Mutex
  - ファイル名、ファイルパス
  - レジストリ

  etc.




## Yaraルール

```
rule CrowdStrike_CSIR_12024_01 : deep_panda derusbi mygeeksmail artifacts
{
        meta:
                weight = 100
                copyright = "CrowdStrike, Inc."
                description = "Strings in Derusbi malware, decoder available
in report"
                version = "1.0"
                last_modified = "2013-04-04"
                actor = "DEEP PANDA"
                report = "CSIR-12024"
                malware_family = "Derusbi, MyGeeksmail"
                in_the_wild = true
        strings:
                $isapi  = "ISAPI_CONNECT"
                $pcsock = "PCC_SOCK"
                $pcc    = "PCC_PROXY"
                $webprox= "PCC_WEBPROXY"
                $obwidget1 = { C1 F8 0? 32 C? 88 04 2e 46 }
                $obwidget2 = { E8 ?? 1? 00 00 32 C? 88 04 2E 46 }
        condition:
                2 of them
}
```




## Snortルール

```
alert tcp any any <> any any (msg: “BackDoor Beacon Attempt”; content:”|78 7c 71 4c 4a 49 49 49
4A 4C 46|”; classtype:backdoor; sid:123456; rev:27122011;)

alert tcp any any <> any any (msg: “BackDoor Beacon Attempt”; content:”Google”; http_uri;
classtype:backdoor; sid:123457; rev:27122011;)

alert ip 1.9.5.38 any <> any any (msg: “Malicious Host Detected”; classtype:backdoor; sid:123460;
rev:27122011;)

alert tcp any any <> any any (msg:”BackDoor Beacon Attempt”; content:”|03 01 74 80 82 21 b5 64
c2 74 22 e3 02 00 00 00 49 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00|”; classtype:backdoor;
sid:123458; rev:27122011;)

alert ip 202.86.190.3 any <> any any (msg:”Malicious Host Detected”; classtype:backdoor;
sid:123459; rev:27122011;)

alert tcp any any <> any any (msg: “BackDoor C2”; content: “POST /forum/login.cgi HTTP/1.1”;
content:”User-Agent: Mozilla/4.0”; classtype:backdoor; sid:123461; rev:27122011;)

alert tcp any any <> any any (msg: “BackDoor C2”; content: “GET /Photos/Query.cgi?loginid=”;
classtype:backdoor; sid:123462; rev:27122011;)

alert tcp any any <> any any (msg: “BackDoor C2”; content: “POST /Catelog/login1.cgi HTTP/1.1”;
content:”User-Agent: Mozilla/4.0”; classtype:backdoor; sid:123461; rev:27122011;)
```




## Indicator Hierarchy


**Adversary**

**（攻撃者＝TTPs）**

IPアドレス
難読化手法
C2サーバ
エクスプロイト（攻撃コード）
配送方法
マルウェア・ハッシュ値

## FireEye + Yara





## コンピュータ・フォレンジック

- **PC内の様々なデータからタイムラインを作成し、全体を俯瞰しながら、あたりを付けて、解析していく。**
- **調査個所**
  - 攻撃者の作業領域 （C:¥Users¥<username>¥AppData¥Local¥Temp など）
  - Master File Table （$MFT）
  - INDXファイル （$I30）
  - Prefetchファイル （C:¥Windows¥Prefetch¥）
  - 代替データストリーム （ADS）
  - Web閲覧履歴
  - レジストリ （ASEP、UserAssist、MUICache など）
  - イベントログ
  - メモリ

  など。。。

調査個所が多岐に渡り、高い専門性が必要。




## コンピュータ・フォレンジックの課題

- **現場の課題**
  - 専門性が高く、自社でスキルを持った社員をかかえるのは困難。（ファイルシステム、レジストリ、メモリダンプ、イベントログ等の解析スキルが必要。）
  - 感染の疑いのあるPCが多数存在する。
  - 感染端末が遠隔地にある場合、対応が難しい。
  - 既に痕跡が消えている。
- **アンチ・コンピュータ・フォレンジック（攻撃者が使うテクニック）**
  - 暗号化などのデータ秘匿。
  - マルウェアの自己消去。
  - ログの消去。
  - タイムスタンプの改ざん。（Timestompなどのアンチフォレンジック・ツール）
  - フォレンジック行為を検知する機能が実装されたマルウェア。




## ETDRとは

- **ETDR = Endpoint Threat Detection and Response Tools**
- **エンドポイント端末にインストールするエージェントで、下記二つの機能を持つ。**
  - 脅威の検知。（エクスプロイト、マルウェア、C2通信などを発見）
  - フライトレコーダ機能。（プログラムの実行、レジストリの変更、通信状況などを記録する機能。）


- **ETDRはガートナー社が名付けたカテゴリ。**
  - **http://blogs.gartner.com/anton-chuvakin/2013/07/26/named-endpoint-threat-detection-response/**
  - **http://blogs.gartner.com/anton-chuvakin/2013/08/05/endpoint-threat-detection-response-deployment-architecture/**

## ETDRの強み

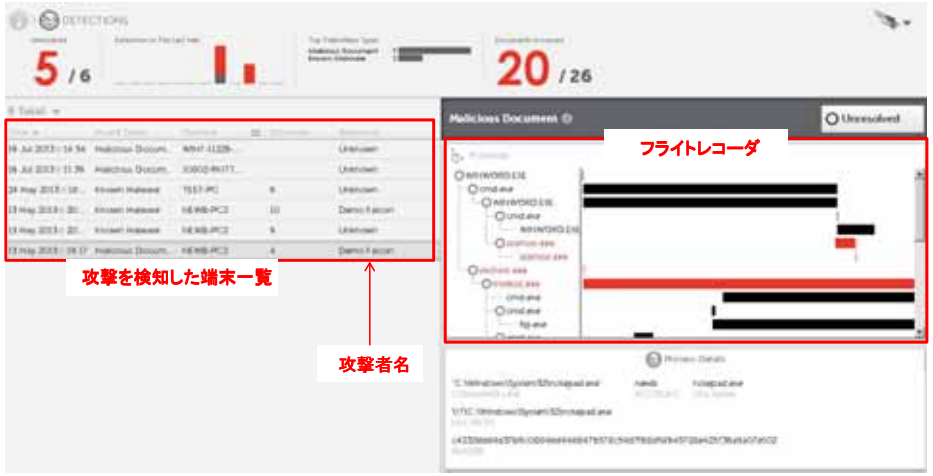
- インシデント発生時における証拠保全のプロセスが不要になる。
- コンピュータ・フォレンジックに必要な情報がいつでも素早く閲覧できる。
  - レジストリの変更履歴
  - プログラムの実行履歴
  - 通信の履歴
  - 脅威の発生履歴

  など。
- PC内のデータでタイムスタンプが改ざんされても、ETDRで取得されたデータには影響ない。
- 多くの端末を横断的にフォレンジックできる。

コンピュータ・フォレンジックの世界で、イノベーションが起きるか？




## CrowdStrike Falcon Host 管理画面　その1







## CrowdStrike Falcon Host 管理画面　その2

- プロセスの詳細


- アクセスされたファイル




## CrowdStrike Falcon Host 管理画面　その3

- VTの結果


- 通信先の特定

## ご清聴ありがとうございました。

研究センターのブログを開設！

**http://blog.macnica.net/**

世界の最新セキュリティ技術や動向を紹介！