標的型攻撃の実態と対策アプローチ 第6版

日本を狙うサイバーエスピオナージの動向2021年度

2022年6月15日
株式会社マクニカ
TeamT5

目次

はじめに

マクニカでは、セキュリティ研究センターを中心に、2014年から、日本に着弾する標的型攻撃（サイバーエスピオナージ）を分析してきました。情報窃取を目的とした、この種のサイバー攻撃は、ランサムウェアによる攻撃と違い、長期間に渡って侵害に気づかない組織が多く、表面化するケースも比較的少ないため、情報共有がされにくいと言えます。

しかし、国内外のサイバーセキュリティ業界の長年の努力によって今日までに収集された攻撃痕跡（マルウェア、攻撃インフラ、ログ）を分析していくと、各攻撃グループのTTPs、目的や意図、スキルレベルなどが、徐々に浮き彫りになってきています。このような取り組みは、組織を超えた戦略的な情報共有とインテリジェンスへの昇華によって成り立ちます。今回で第6版となる「標的型攻撃の実態と対策アプローチ」ですが、第4版から、台湾のTeamT5社と共同で分析と執筆を行っています。標的型攻撃（サイバーエスピオナージ）は地政学リスクや国家間の緊張関係に大きく依存するため、そのような意味でも、台湾のTeamT5社との協業には大きな意味と意義があります。

本レポートでは、2021年度（2021年4月から2022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関する分析内容を、注意喚起を目的として記載しています。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。レポートの最後には、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。

日本企業の産業競争力を徐々に蝕んでいく標的型攻撃に対して、今後も粘り強い分析と啓蒙活動に取り組んでいく所存です。

攻撃のタイムラインと攻撃が観測された業種

2021年度の攻撃動向は、2020年度の観測[1]から継続してAPT10攻撃グループのLODEINFOマルウェア[2]を使った攻撃とSodaMasterマルウェア[3] [4]を使ったA41APT攻撃キャンペーン[5] [6]が継続して活発に観測されました。A41APT攻撃キャンペーンでは、攻撃に利用される主なペイロードがSodaMasterと新たに観測されたJackpotの2種類となりました。また、昨年度の観測では活動が低下していましたが、BlackTech攻撃グループの攻撃が観測されました。ただし、BlackTech攻撃グループの標的は、国内企業ならびにその中国拠点を最初の標的にしていたと思われます。BlackTech攻撃グループは、これまで国内ではPLEADやTsCookieマルウェアによる攻撃観測が多く見られましたが、Flagpro[7]やSpiderRATといったマルウェアが観測されています。また、APT38攻撃グループのバックドア[8]を使った攻撃が国内で発生していたと思われます。全体的に、攻撃グループ数が6グループから4グループへ、攻撃キャンペーンもこれまで10程度のキャンペーン数から7と攻撃は減少傾向です。

表 1. タイムチャート

1. https://www.macnica.co.jp/business/security/manufacturers/files/mpressioncss_ta_report_2020_5.pdf
2. https://blogs.jpcert.or.jp/ja/tags/lodeinfo/
3. https://blog.kaspersky.co.jp/apt10-sophisticated-multi-layered-loader-ecipekac-discovered-in-a41apt-campaign/30393/
4. https://blog.trendmicro.co.jp/archives/29842
5. https://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_202_niwa-yanagishita_jp.pdf
6. https://jsac.jpcert.or.jp/archive/2022/pdf/JSAC2022_9_yanagishita-tamada-nakatsuru-ishimaru_jp.pdf
7. https://insight-jp.nttsecurity.com/post/102h7vx/blacktechflagpro
8. https://securelist.com/the-bluenoroff-cryptocurrency-hunt-is-still-on/105488/

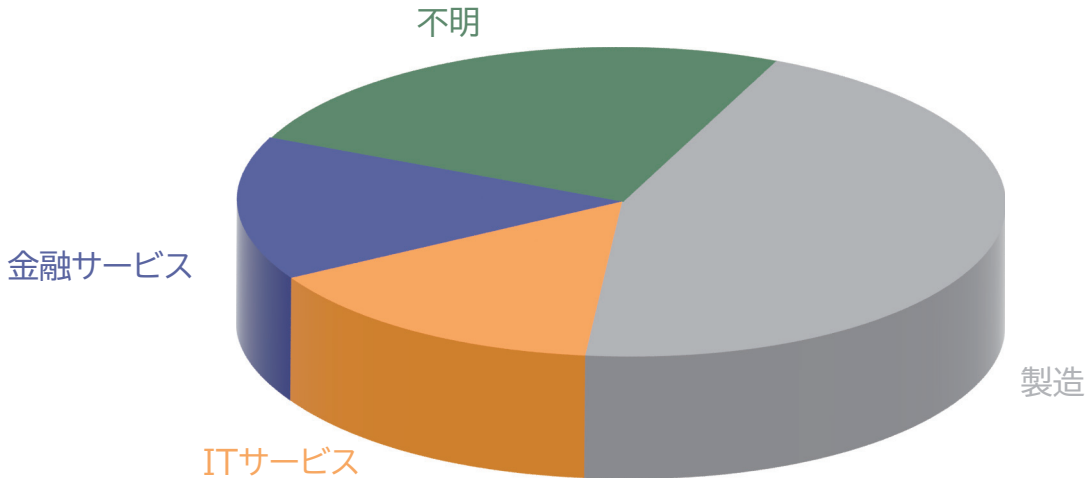


図1. 標的組織の割合（2021年度）

年間を通して、APT10のSodaMasterを使った攻撃が製造業で観測されました。また、これまで主にメディアを標的としてきたLODEINFOを使った攻撃が製造業でも観測されたため、製造業での標的型攻撃の観測割合が顕著に大きくなっています。それ以外の業種では、ITサービス、金融サービスがほぼ同じ割合を占めています。また、検体としては入手したものの、APT10のLODEINFOなどで標的がはっきりしないものもあり、不明の割合が増えています。SodaMasterを使った攻撃キャンペーンでは、マルウェアが設置されたホストは、すべて海外拠点のWindowsサーバでした。BlackTech攻撃グループは、ITサービス関連などへの攻撃が見られましたが、これは中国拠点への感染を狙った活動が活発であったと思われます。そのため、国内企業の海外拠点からの侵入が増加傾向です。攻撃手法については、以降のセクションで記載しますが、感染を狙ったスピアフィッシングメールに添付されたOfficeのマクロファイル、遠隔操作マルウェアとして利用されるペイロードがC2と通信して任意のコマンドや操作を行うといった本質的なところでの手法の変化や目新しさはなく、現在のセキュリティ技術では既に検出は難しくないと思われます。しかしながら、攻撃者はその検出技術が適用されていない守りの手薄な海外などの拠点を攻撃して国内企業の知財・情報の窃取を試みていると思われます。

ここに記載した業種では、できれば関連会社や海外含む各拠点で、本書の後半で記載する検出手法を参考に確認や対策の検討を行って頂ければと思います。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。

攻撃の概要

以下は、2021 年 4 月から 2022 年 3 月までの月ごとに観測された攻撃の概要を記載しています。

2021 年 4 月 (製造)

APT10 LODEINFO

APT10 攻撃グループの LODEINFO マルウェアに感染させる事を目的としたスピアフィッシングメールが、製造業で観測されました。スピアフィッシングメールに添付された Microsoft WORD ファイルは、メール本文に記載のパスワードで保護されたものでした。WORD ファイルのマクロを有効にする事で、正規の実行ファイルと LODEINFO マルウェアを含むサイドローディング DLL の 2 つのファイルが書き込まれて実行されます。観測されたバージョンは、v0.4.9(SHA256: f142eecf2defc53a310b3b00ae39ffecc1c345527fdfbfea8ccccd0d69276b41)で、バージョン情報が更新されているものの、遠隔操作コマンドの追加などはありませんでした。

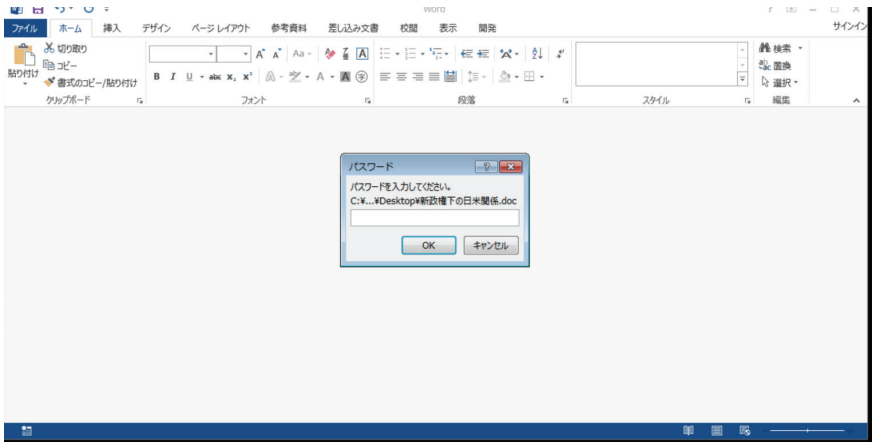


図 2. LODEINFO v0.4.9の感染を狙ったパスワード保護されたドキュメントファイル

2021年6月(金融サービス)

APT38 XorDNS Downloader

パブリックマルウェアリポジトリで検出されたvpsps.dll(SHA256: 546e8bbaf15a81369af11138f933900dfbda8a8fc2c1e6821dbfbcb6498e280d) は、APT38攻撃グループが金融サービス機関への攻撃で利用したダウンローダです。設定ファイルに記載されたドメインの名前解決から得たIPアドレスを固定の4バイト値でXORしたアドレスを真のC2として使う特徴があります。この攻撃グループのこれまでの標的とこのツールの特性から国内の金融サービス関連の組織が攻撃を受けたと思われます。

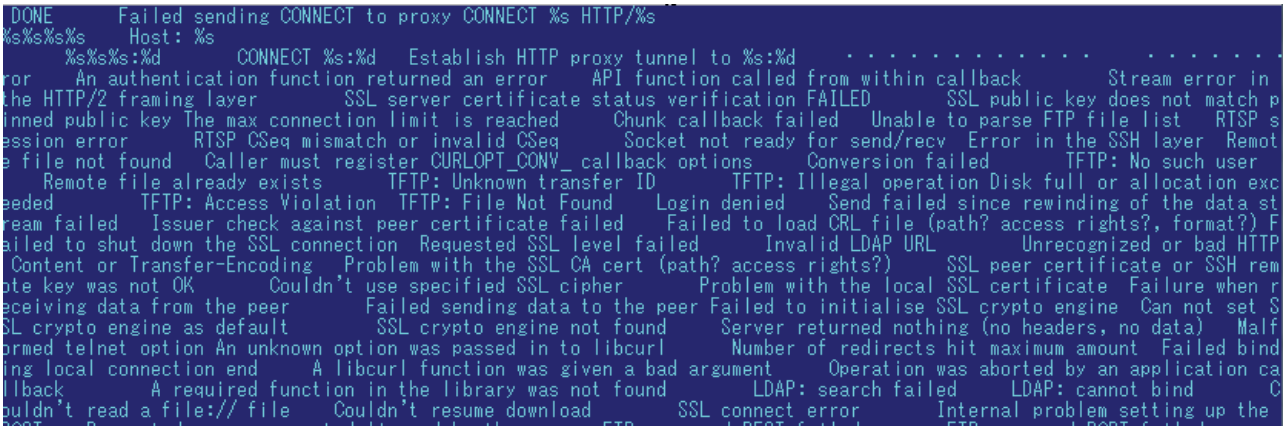
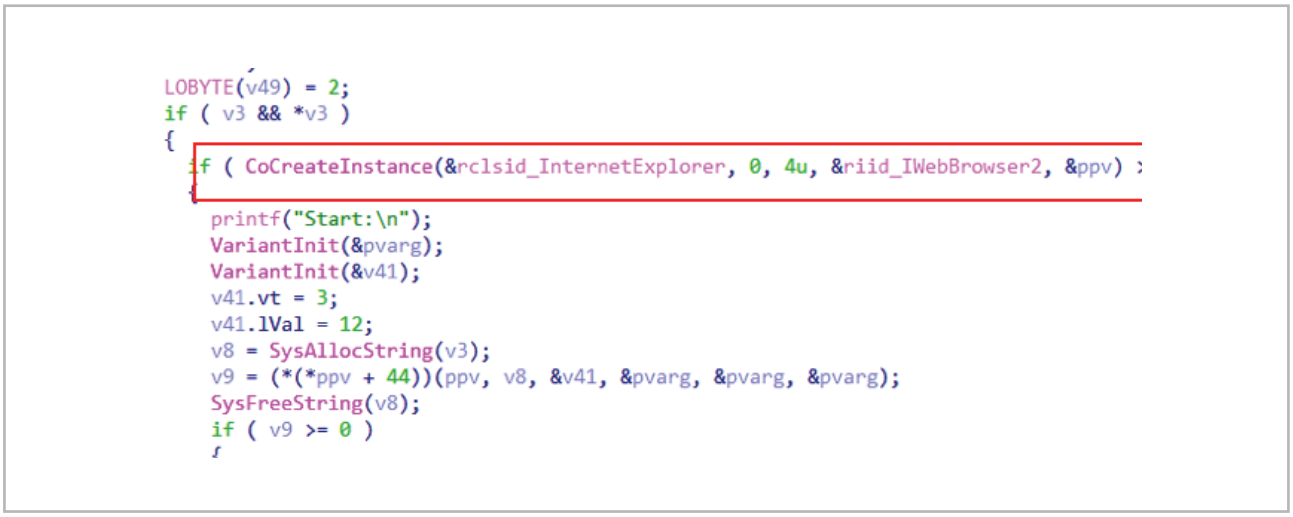


図 3. 検体に含まれている特徴的な文字列

2021年7月(ITサービス)

BlackTech Flagpro

BlackTech攻撃グループによるFlagproダウンローダーへの感染を目的としたスピアフィッシングメールが国内企業の中国拠点で観測されました。メールには、线路信息.xlsm(SHA256: ba27ae12e6f3c2c87fd2478072dfa2747d368a507c69cd90b653c9e707254a1d)が添付され、パスワードによる保護がなされていました。これを解除してマクロを有効化する事で、Flagproマルウェア(SHA256: e197c583f57e6c560b576278233e3ab050e38aa9424a5d95b172de66f9cfe970 / C2: http[:]//139.162.87[.]180/index.html)がディスクに書き込まれ実行されます。Flagproは、COMインターフェース経由でiexploer.exe(Internet Explorer)を使ってダウンロードの通信を行う特徴があります。



```
LOBYTE(v49) = 2;
if ( v3 && *v3 )
{
  if ( CoCreateInstance(&rclsid_InternetExplorer, 0, 4u, &riid_IWebBrowser2, &ppv) >
  {
    printf("Start:\n");
    VariantInit(&pvarg);
    VariantInit(&v41);
    v41.vt = 3;
    v41.lVal = 12;
    v8 = SysAllocString(v3);
    v9 = (*(*ppv + 44))(ppv, v8, &v41, &pvarg, &pvarg, &pvarg);
    SysFreeString(v8);
    if ( v9 >= 0 )
    {
```

図 4. FlagproマルウェアのCOMインターフェースの利用

2021年10月(複数の製造)

APT10 SodaMaster/Jackpot

2021年10月から12月にかけて、APT10攻撃グループのA41APT攻撃キャンペーンの攻撃が国内

企業の海外拠点を中心に活発に観測されました。この攻撃キャンペーンの侵入には、昨年度同様に主にSSL-VPN装置の脆弱性が悪用され、遠隔操作で利用されるペイロードSodaMasterは、これまで観測されていたdflsのコマンド識別子がアップデートされ、cからxまでのコマンドが実装されていました。また、WindowsのIISサーバでは、遠隔操作のコマンドが成功した際にJackpotの文字列を返す特徴のあるJackpotと名づけられたウェブシェルのように動作するペイロードも観測されました。

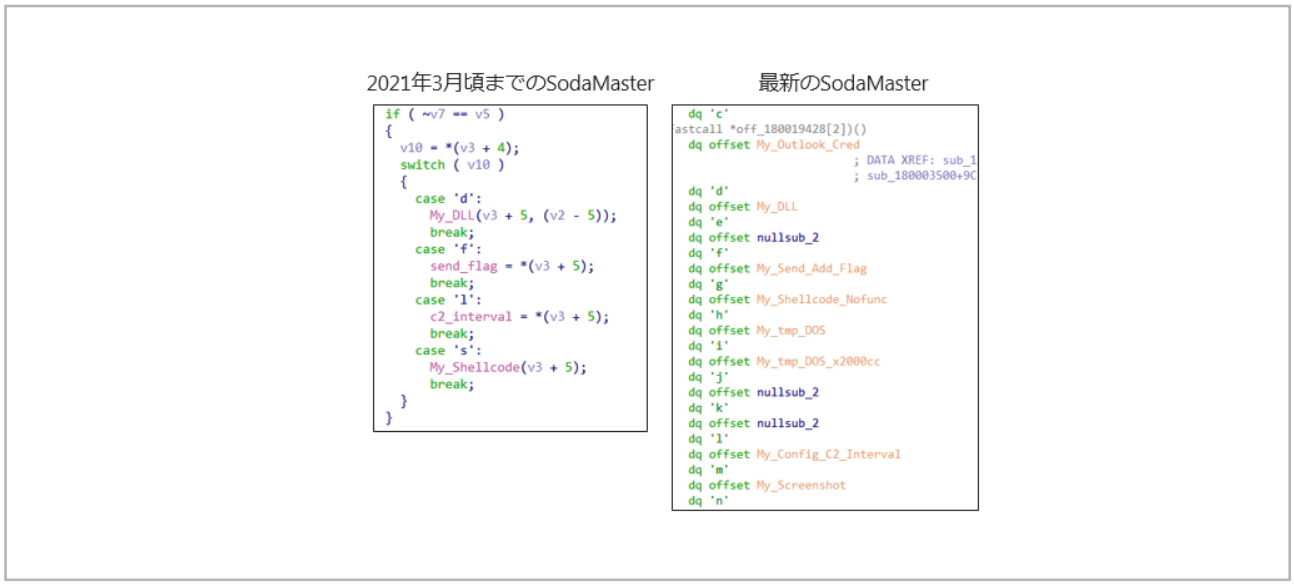


図 5. SodaMasterマルウェアに追加されたコマンド識別子

2021年11月(不明)

BlackTech Spider RAT

BlackTech攻撃グループによるSpider RATへの感染を目的としたスピアフィッシングメールが観測されました。メールには、2021-10工资中公积金问题咨询.xlsm(SHA256: 0911e5d1ec48430ff9a863f5c4a38f0c71872d8bd6c89f07d6ae16d78eca162f)が添付され、マクロを有効化する事で、Spider RATマルウェア(SHA256: 8c3df0e4d7ff0578d143785342a8033fb6e76ce9f61c2ea14c402f45a76ab118 / C2: centos.onthewifi[.]com)がディスクに書き込まれ実行されます。Spider RATは、HTTPSで外部サーバと通信を行い、リモートからの任意のコマンドとファイルダウンロードなどの操作が可能なRATです。検体にはデバッグを目的としたメッセージ出力が残されています。

```
v5[76] = 0i64;
v5[76] = beginthreadex(0i64, 0, aa_Work, v5, 0, ThrdAddr);
v6 = *&a1[1].config.data1[4];
if ( *(v6 + 16) )
{
  if ( !sub_1400042A0(v6, 0i64, 1i64, 0i64, 0, 2048, Src) )
  {
    v14 = 15i64;
    v13 = 0i64;
    v12 = 0;
    aa_message(v11, "pWork->HC->HttpSendMessage failed!", 34ui64);
    sub_140002DB0(v11);
  }
  v10 = 0;
  *&a1[1].config.c2[108] = beginthreadex(0i64, 0, aa_handle_c2_command, a1, 0, &v10);
  while ( *(*&a1[1].config.data1[4] + 16i64) )
    Sleep(5000u);
}
```

図 6. Spider RATに特徴的なデバッグ文字列

2021年12月(不明)

APT10 LODEINFO

APT10攻撃グループのLODEINFOマルウェアに感染させる事を目的としたスピアフィッシングメールが観測されました。スピアフィッシングメールに添付されたMicrosoft WORDファイルのマクロ機能を有効にする事で、正規の実行ファイルとLODEINFOマルウェアを含むサイドローディングDLLの2つのファイルが書き込まれて実行されます。観測されたバージョンは、v0.5.6で、3つのコマンドが追加され、遠隔操作コマンドの識別文字列(command, ls)などがxorでエンコードされるなど、解析を阻害するようになりました。

```
_0 db 'Supported commands:',0Dh,0Ah
db '[1] command',0Dh,0Ah
db '[2] ls',0Dh,0Ah
db '[3] rm',0Dh,0Ah
db '[4] mv',0Dh,0Ah
db '[5] cp',0Dh,0Ah
db '[6] cat',0Dh,0Ah
db '[7] mkdir',0Dh,0Ah
db '[8] send',0Dh,0Ah
db '[9] recv',0Dh,0Ah
db '[10] memory',0Dh,0Ah
db '[11] kill',0Dh,0Ah
db '[12] cd',0Dh,0Ah
db '[13] ver',0Dh,0Ah
db '[14] print',0Dh,0Ah
db '[15] ransom',0Dh,0Ah
db '[16] keylog',0Dh,0Ah
db '[17] ps',0Dh,0Ah
db '[18] pkill',0Dh,0Ah
db '[19] comc',0Dh,0Ah
db '[20] autorun',0Dh,0Ah
db '[21] config',0Dh,0Ah,0
```

図 7. LODEINFOマルウェアv0.5.6でサポートするリモートコマンド

2022年3月(不明)

APT10 LODEINFO

LODEINFOのバージョン0.5.9に感染させるドキュメントファイルが観測されました。対解析手法、遠隔操作コマンドという点では、v0.5.6から変化はみられませんが、DLL Side-Loadingで悪用される正規

ファイルの変更やC2サーバ接続失敗時にFirefoxに設定されたプロキシ情報を使う処理の追加がされています。

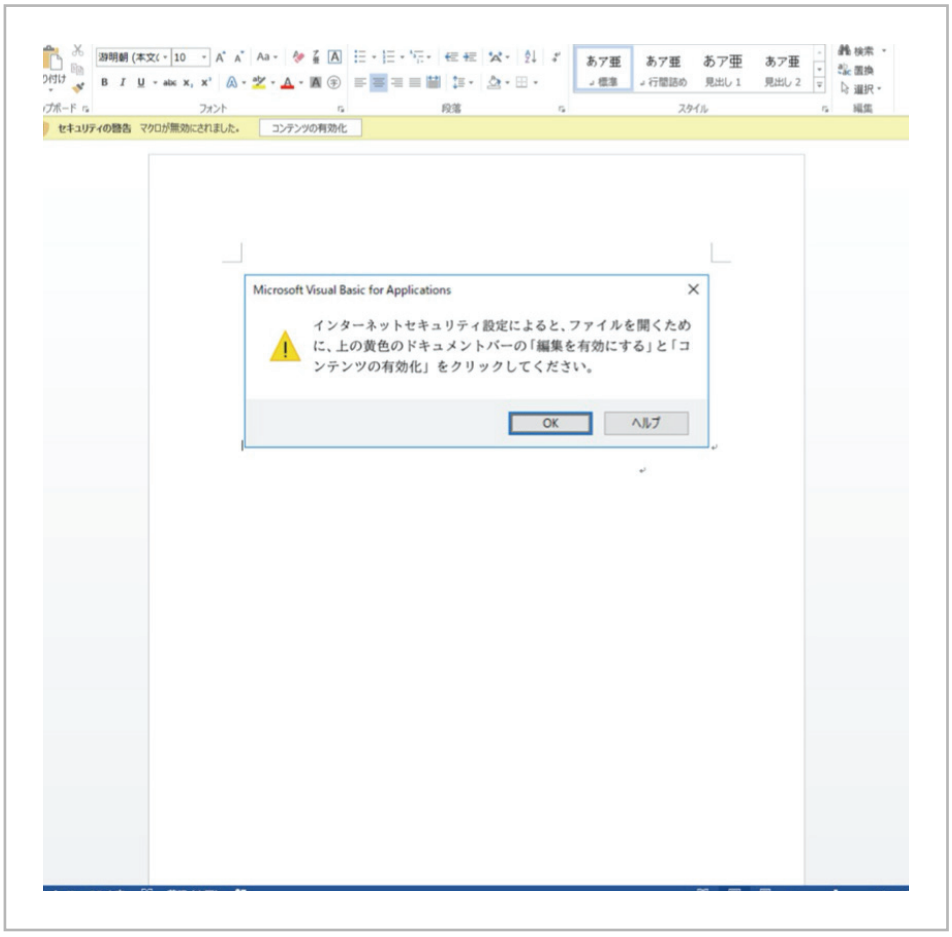


図 8. LODEINFOマルウェア v0.5.9に感染させるドキュメントファイル

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。

APT10（SodaMaster/Jackpot）

攻撃の全体像

観測されている攻撃のケースでは、管理体制の脆弱な海外拠点のSSL-VPN装置の脆弱性を攻撃して侵入します。組織のネットワークに侵入した後は、RDPとSMBのポートスキャンを行い、ポートの開いているPCのRDPやSMBに対して、窃取したクレデンシャルを使ってログオンを試みます（SSL-VPN装置の脆弱性によっては、SSL-VPN装置からクレデンシャルが窃取できるものがあります）。窃取したクレデンシャルでログオンできない場合は、パスワードを変えながら総当りでSMBの接続を試みます。ここで、RDP接続可能なシステムはWindowsサーバが多く接続に成功した場合には、このサーバを攻撃の長期の足場とするために、正規実行ファイルとDLLサイドローディングのローダーDLL（SigLoader）、ならびに暗号されたペイロードが含まれたファイルを同じディレクトリに保存し、タスクスケジューラーで正規実行ファイルが起動するように設定して永続化を図ります。これらのファイルは、4個から5個のファイルからなり、C:¥Windows¥（サブフォルダ含む）配下に設置される特徴があります。C:¥Windows¥配下にマルウェアをインストールする特徴は、2022年1月までの観測では、A41APT攻撃キャンペーンで一貫していると思われます。

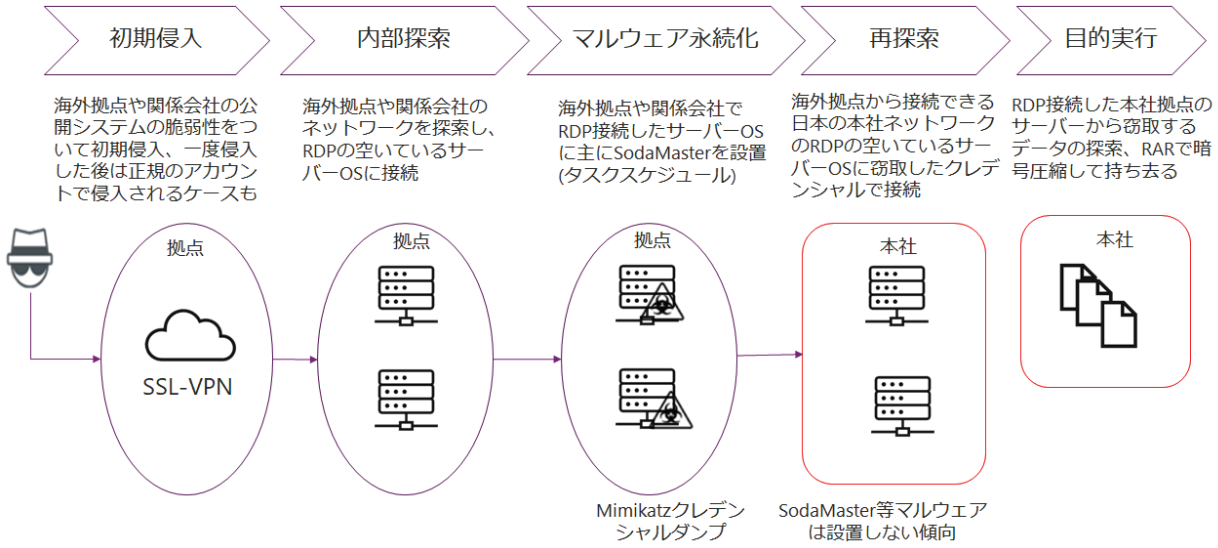


図9. A41APT攻撃キャンペーンの全体像

SigLoaderから起動されるメモリ上のペイロードは、2021年の観測ではSodaMasterと呼ばれるペイロードが主になっています。2020年までの観測では、それ以外にxRAT、Cobalt Strike Stager Shellcode、P8RATが観測されています。足場となるマルウェアをインストールするサーバOSの台数は

各拠点で1-2台程度と台数が少なく、侵入の痕跡を消去するためにイベントログを削除する特長があります。また、この拠点のシステムから更に侵入を拡大するために、Mimikatzを使ったクレデンシャルダンプやWinRARでWindows上のOfficeやテキストといったファイルを窃取して持ち去り、更なる侵入拡大のクレデンシャル情報を入手します。攻撃が観測された組織では、ヨーロッパの異なる複数の国、東南アジアの複数の国で攻撃が観測されており、初期侵入の地域性はなく標的とした日本組織の侵入可能な拠点は標的にしていると思われます。各拠点で足場を構築した後、csvdeツールでドメインの情報を収集し、日本の本社地域のサーバに同様に窃取したクレデンシャルでRDP接続を試みます。日本本社のサーバにRDPでの接続に成功した場合、日本本社のサーバには、SigLoaderやSodaMasterといったマルウェアは設置しない傾向があります。攻撃者は、WMIを使ってリモートシステムにインストールされているセキュリティソフトウェアを把握していると思われ、近年EDR等でセキュリティが強化された日本のシステムにはマルウェアの設置を避けている節があると思われます。日本の本社セグメントのWindowsサーバOSから参照可能なファイルやファイルサーバーへ接続を行い、現在のところ無作為にファイルを収集してRARで暗号圧縮して窃取していると思われます。

SigLoaderの概要と検出

正規実行ファイルから、Side-LoadingされるDLLファイルです。同じフォルダに設置されたDLLファイルからデジタル署名の末尾に追加された暗号データを読み、これを独自に実装されたAES、DESとXORのアルゴリズムの組み合わせで復号します。復号には、3つのアルゴリズムのすべてが使われるケースはまれで、DESとXORやXORとAESの組み合わせが多く、様々に実装されています。SigLoaderは、読み込んだファイルの暗号データを復号してシェルコードとメモリ上のSigLoaderとして展開し、展開されたメモリ上のSigLoaderがまた別のファイルの暗号データを読んで復号し、ペイロードをロードするシェルコードとペイロードに展開されます。また、2021年の観測では、検体のコンパイル時間の改ざん、AESのモード変更、2020年の検体に比較的多く見られたOutputDebugString()の多用がなくなるなどコードにアップデートがありました。

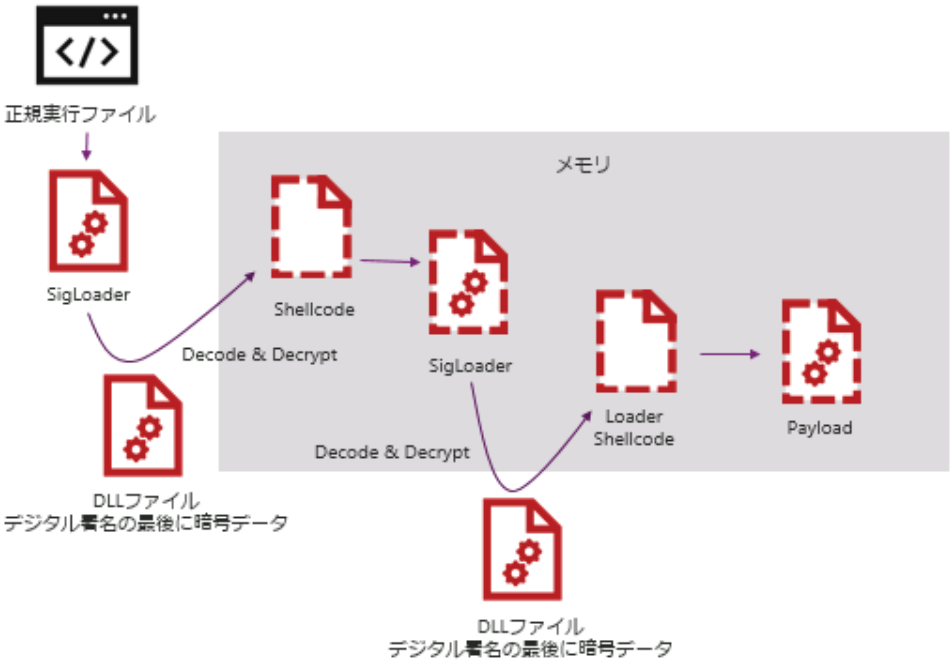


図10. SigLoaderのペイロード展開フロー

2020年にパブリックリポジトリにアップロードされたSigLoaderの検知率は2ヶ月に渡りほぼ未検出となっていましたが、2021年に観測されたSigLoaderはアップロードされた時点から検出できるベンダーがあり、検知率は低いものの脅威としては2020年に多く攻撃観測されたときより低下していると思われます。

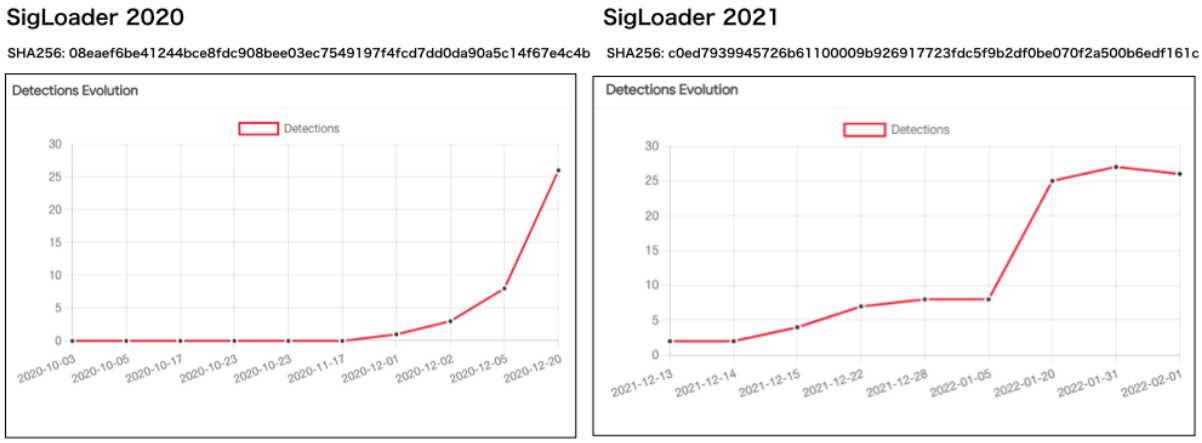


図11. SigLoaderの検出率

SigLoaderは、C:¥Windows¥(サブフォルダ含む)配下にタスクスケジューラーで起動するように設定された3rd Partyの正規実行ファイルからロードされる特徴があります。このフォルダでかつタスクスケジュール起動する3rd Partyのプログラムはまれなため、主に対策の手薄な拠点などは次のコマンドを各Windowsサーバで実行し、起動するプログラムがないかどうか確認する事も検出に有効です。

>schtasks /query /fo list /v | findstr C:¥Windows¥

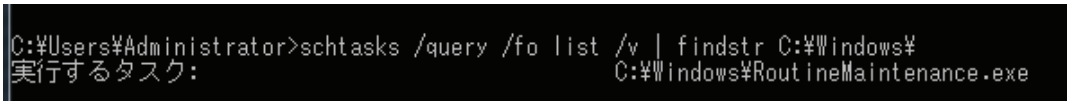


図12. SigLoaderをロードする正規実行プログラムの検出

SodaMasterの概要と検出

SodaMsterは、SigLoaderからメモリに展開されるペイロードの1つです。バージョンによって異なりますが、ds、dfls、c-xと、dとsの命令を持つ事が特徴のペイロードです。主にメモリ上にダウンロードしたDLLを実行するd、メモリ上にダウンロードしたシェルコードを実行するsの命令で遠隔操作をしていると思われます。SodaMasterは、2021年にHUI Loaderと名づけられたSigLoaderとは別のローダーからメモリに展開して実行された事が観測されており、APT10のSigLoaderとセットで使われるケースの他に、中国を拠点とした別の攻撃グループが攻撃ツールとして利用を開始したと思われます。SodaMasterがペイロードとして観測された攻撃のケースでは、SodaMasterが動作するプロセスの引数にMimikatzのコマンド引数が観測されたケースがあり、SodaMasterがメモリにダウンロードするモジュールとして、Mimikatzをファイルとして保存せずに攻撃に利用するケースがあると思われます。EDRのようなコマンド引数も含めて監視の行えるセキュリティツールでは、Mimikatzの特徴的なコマンドライン sekurlsa::logonpasswords などを監視対象の文字列として攻撃のモニタリングを行う事で攻撃の検出が行えます。

Jackpotの概要と検出

Jackpotは、SigLoaderからメモリに展開される2021年に初めて観測されたペイロードです。1から10までの遠隔操作のコマンドを持ち、遠隔操作の命令に成功した際にJackpotの文字列を返す特徴があります。観測された環境ではWindowsのIISサーバで動作していました。Jackpotは、ウェブシェルのように動作しますが、小さなシェルプログラムではなく、C/C++で開発されたサイズのあるプログラムです。その他に、ウェブシェルと違い、ウェブサーバー上でウェブページのファイルなしでリスニングして攻撃者からの命令通信を待ちます。また、IISのサーバで動作する場合、IISと同じポートで待ち受けする別のウェブサービスプログラムとなります。この場合、Jackpotの待ち受けURLページへのアクセスは、IISのアクセスログに残らず、ウェブシェルの様に待ちうけのウェブページのファイルも存在しないため、通常のウェブ侵害の調査アプローチでは検出が難しいかもしれません。一方で、ウェブシェルとしての任意の操作が行われるため、SodaMasterと同様にプロセスの実行コマンドを監視する、SigLoaderの検出やタスクスケジューラーからハンティングするといったアプローチでの検出が有効だと思われます。

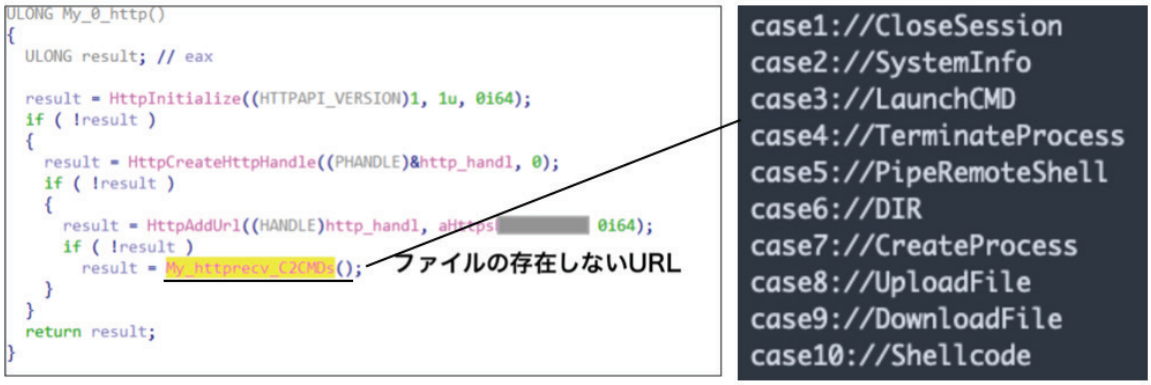


図13. Jackpotの待ちうけコードとコマンド識別子

LODEINFOを使う攻撃キャンペーン

2019年末からLODEINFOと呼ばれるバックドアを使った攻撃活動が観測されていますが、攻撃グループは2021年度もLODEINFOを改良し新しいバージョンの投入を続けました。弊社で観測したバージョンは、0.4.9、0.5.6、0.5.9ですが、本レポート執筆時点で最新バージョンの0.6.2の観測情報も公開されています[9]。過去観測した標的業種は日本の研究機関やメディアでしたが、2021年は製造業への攻撃も観測しました。このことから攻撃グループの目的に安全保障関連だけでなく製造業の知財窃取も含まれるようになった可能性があると考えています。

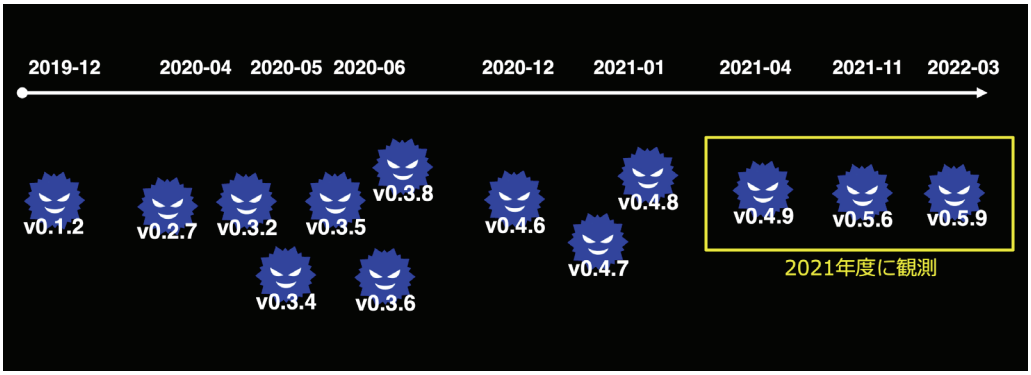


図 14. LODEIFNOのタイムライン

旧バージョンからの変更

v0.4.9では旧バージョンからの大きな違いは見られませんでしたが、v0.5.6では”comc”、”autorun”、”config”のコマンドが追加されました。

表 2. LODEINFO リモートコマンド一覧(v0.5.6時点)

コマンド名	機能
command	LODEINFOがサポートしているコマンド表示
ls	ファイル一覧
rm	ファイル削除
mv	ファイル移動
cp	ファイルコピー
cat	ファイルの内容表示
mkdir	フォルダ作成
send	感染機器へファイルをアップロード
recv	感染機器からファイルをダウンロード
memory	シェルコードを他プロセスへインジェクト
kill	プロセス終了
cd	指定フォルダへ移動
ver	LODEINFOバージョン情報表示
print	スクリーンキャプチャ
ransom	ファイル暗号化
keylog	キーロギング
ps	プロセス一覧の表示

9. https://twitter.com/jpcert_ac/status/1515940912173502464

pkill	プロセス名指定でのプロセス終了
comc	任意のコマンド実行(WMIを使用)
autorun	自動起動の設定(レジストリ、スタートアップファルダ)
config	v0.5.6時点で未実装(設定情報の表示機能とみられる)

また耐解析が目的とみられますが、コードで使われる文字列の多くがXORでエンコードされるようになりました。C2サーバ間の通信プロトコルでは、v0.5.6以降LODEINFOからC2サーバへデータをアップロードする際に新たにヘッダー部を暗号化するステップが追加されています。

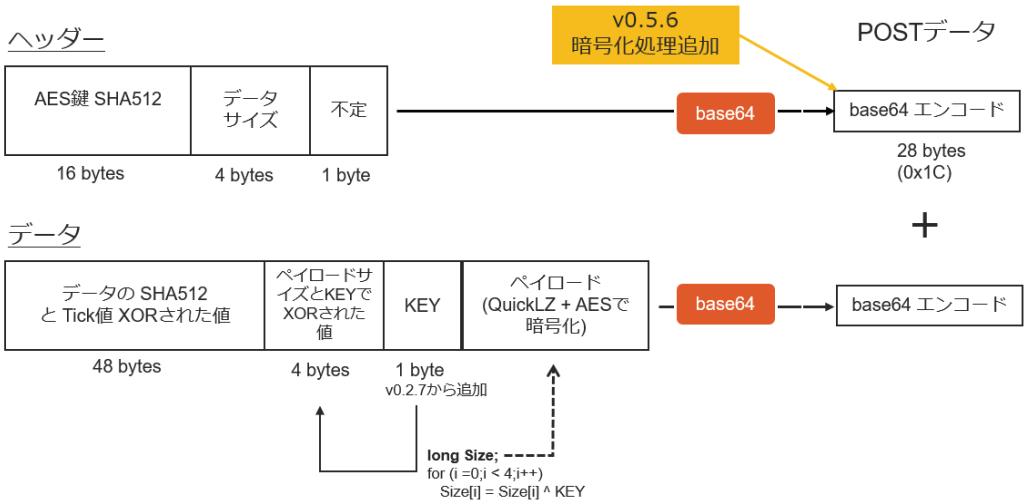


図 15. アップロード通信暗号化手順

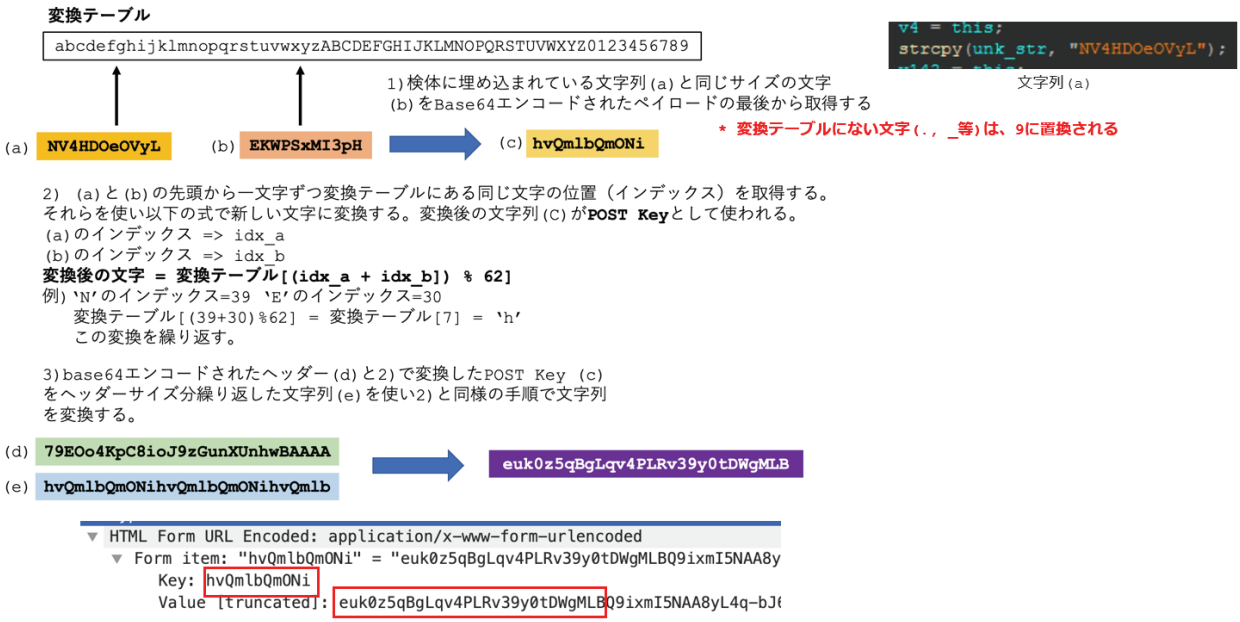


図 16. 追加された暗号化処理

初期アクセス(Initial Access)から永続化(Persistence)までのTTPは、スピアフィッシングメール、マクロの悪用、RUNレジストリキー追加と変化は見られていません。
LODEINFO v0.5.9に感染させるドキュメントファイル
(SHA256: fde82dcccd471b63f511c6f76dc04e12334818cda8b38f5048b8ad85c9357089)
では、ドキュメントファイルのマクロは、マクロとは別のUserForm1に主要な文字列が設定されており、マクロを有効にすると正規の実行ファイルとLODEINFOのローダであるDLLファイルがドロップ・実行されます。
ドロップされる場所: C:¥Users¥Public¥TMWJPA

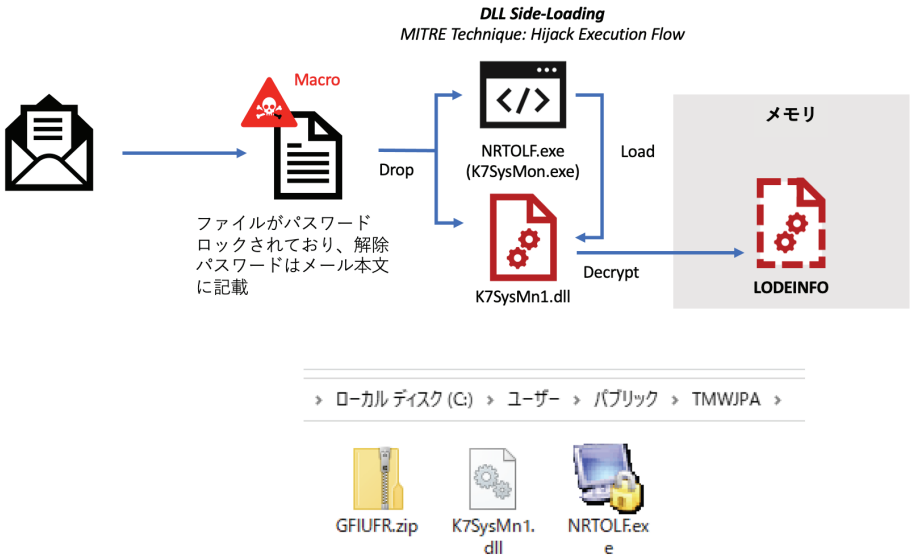


図 17. LODEINFOを使った攻撃フロー

```
Private Sub Document_Open()
Dim SIKHBENAX() As Byte
UGCENLCYI = UserForm1.TextBox1.Text
If Not Dir(UGCENLCYI, vbDirectory) = vbNullString Then GoTo MNOTVAUKO
Debug.Print "VWSCVFVARAXP": MkDir (UGCENLCYI)
YLASDJXOV = UserForm1.TextBox5.Text
NWTHAYFMB = UserForm1.TextBox6.Text
DTIQGQXWQ = UserForm1.TextBox10.Text
With CreateObject(YLASDJXOV).createElement("W")
        .dataType = NWTHAYFMB
        .Text = DTIQGQXWQ
        SIKHBENAX = .nodeTypedValue
End With
TUDIDIDYV = UserForm1.TextBox2.Text
Debug.Print "SDCFEPOHL": TUDIDIDYV = UGCENLCYI & TUDIDIDYV
Debug.Print "UBSUXVDYE": Open TUDIDIDYV For Binary As #15
Debug.Print "GXALJHMKF": Put #15, , SIKHBENAX
Debug.Print "MULTRIHSR": Close #15
XUJPSBTSB = UserForm1.TextBox8.Text
Set JKNLXUCKM = CreateObject(XUJPSBTSB)
Set UVBQFUTDB = JKNLXUCKM.Namespace(TUDIDIDYV).items
JKNLXUCKM.Namespace(UGCENLCYI).CopyHere (UVBQFUTDB)
FJQAHXBVM = UserForm1.TextBox9.Text
Dim OEAFCPGDA
Debug.Print "WNTFONHDSGAE": OEAFCPGDA = Shell(FJQAHXBVM, 0)
ActiveDocument.Paragraphs(1).Range.Delete
Debug.Print "EGMLFBUFQ": ActiveDocument.Content.Font.TextColor = wdColorBlack
Debug.Print "IWLPSOXUQEKB": ActiveDocument.Content.Font.Size = 9
Debug.Print "QYPYNKQFRWCV": ActiveDocument.Save
MNOTVAUKO:
End Sub
```

図 18. v0.5.6とv0.5.9マクロ本文

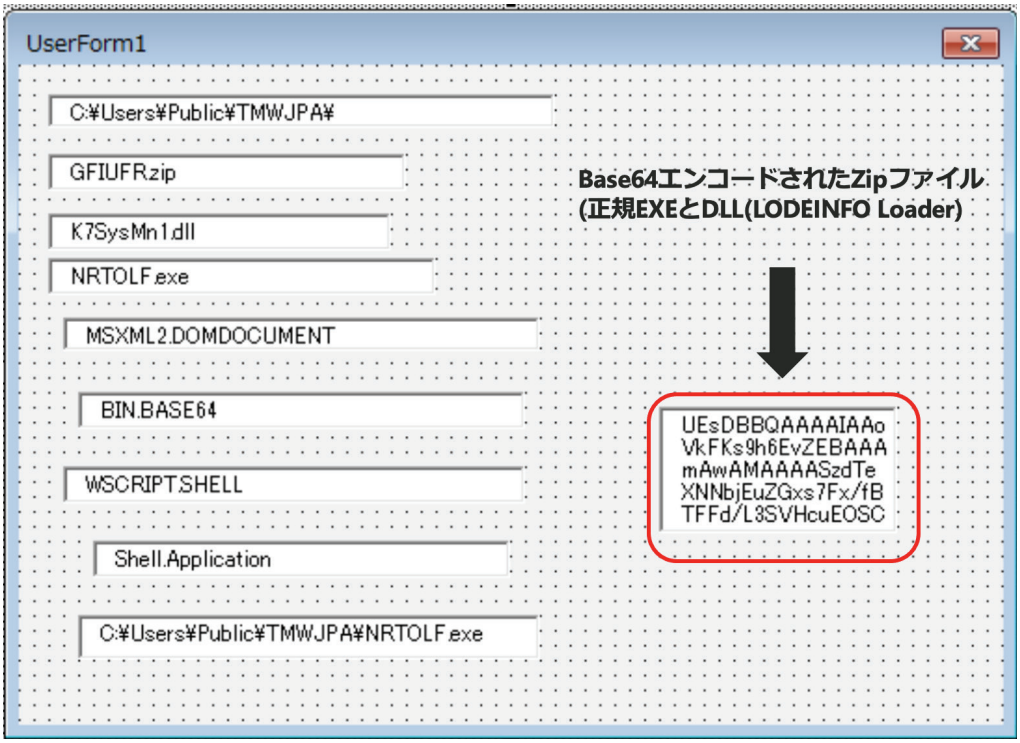


図 19. 主要な文字列が設定されているユーザフォーム

v0.5.9では、以前DLL Side-Loadingテクニックでベースとしていた SfsDll32.dllではなく新たにセキュリティベンダーK7Computing社の正規実行ファイルがロードするDLL ”K7SysMn1.dll”をベースにローダーを開発しています。また、v0.5.9ではC2サーバとの接続が失敗した時にブラウザFirefoxに設定されたプロキシの情報を利用する処理が追加されていました。その読み取りを試みるFirefoxのプロファイルファイルのパスは、ビルトイン アカウントのAdministratorのものが固定で検体に埋め込まれています。このことからプロキシ情報を使う処理がまだ試験的なものであるか、もしくは標的組織ではAdministratorアカウントが有効で、かつFirefoxがデフォルトでインストールされた環境であるのではないかとみています。

```
v96 = this;
v1 = *(aa_get_base_addr() + 0x4010D8);
v102 = v1;
strcpy(path_firefox, "C:\\Users\\Administrator\\AppData\\Roaming\\Mozilla\\Firefox");
path_firefox[55] = 0;
v92 = 1024;
v91 = 1152;
```

図20. LODEINFO検体に埋め込まれているFirefoxのファイルパス

BlackTech 中国拠点を狙った攻撃キャンペーン

2021年度に観測されたBlackTechの攻撃の一つは、日本のITサービス事業者の関連会社へのスピアフィッシングメールです。メールに添付されているドキュメントファイルのマクロを有効にすると“Flagpro”と呼ばれるマルウェアに感染し、新たなマルウェアをダウンロードします。また、標的組織は定かではありませんが、BlackTechが使うマルウェアに感染させる中国語ファイル名のドキュメントファイルが複数存在しており、日本企業の中国拠点または関連会社への侵入を試みる傾向があったのがみられています。

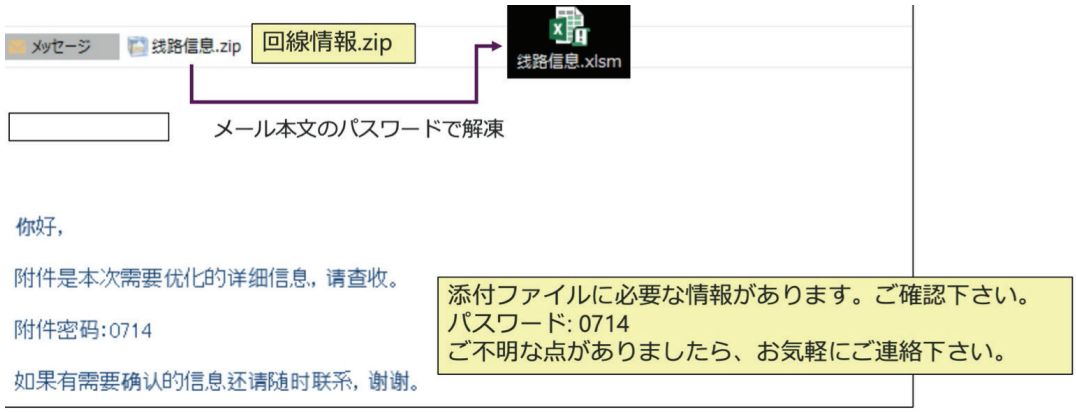


図21. Flagproに感染させるスピアフィシングメール

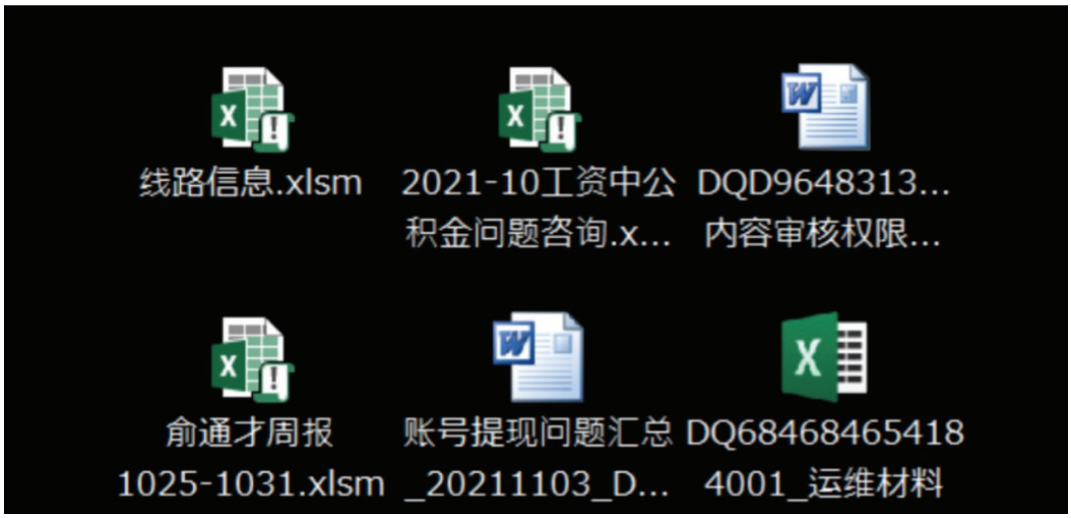


図22. BlackTechが使うマルウェアに感染させる中国語ファイル名のドキュメントファイル

2021年度の活動では、新しいツールセットFlagpro、BTSWindowsRAT、Spider RAT、SelfMakeが使われており積極的に独自ツールを開発・導入しているのが窺われます。

侵入経路

主な手口は、取引先を装ったスピアフィッシングメール、公開サーバ・ネットワーク機器の侵害です。2021年に攻撃者のミスにより外部公開されていたとみられるサーバでCisco、Citrixなどの外部へ公開されるネットワーク製品の脆弱性を悪用するツールが見つかっています[10][11]。また、Exchange Serverの脆弱性ProxyLogonを悪用した情報も公開されています。BlackTechは過去から外部公開機器からの侵入を得意とする攻撃グループで現在も積極的に取り組んでいると考えています。

2020年初頭には、ITサービスプロバイダへの攻撃に使われたとみられるマルウェアとツールを確認しています[12]。このことから組織ネットワークにアクセスする事が可能な業務委託者を侵害し、そこから標的組織に侵入するのもTTPの一つと考えています。

新たな攻撃ツールセット

Flagpro

外部から新たなファイルをダウンロードするダウンローダーです。WindowsのCOM(Common Object Model)を使いInternet Explorerのインターフェース系由で通信を行う特徴があります。HTTPで外部サーバーにアクセスし、サーバからはbase64エンコードされたレスポンスが返ります。レスポンスには、ファイルダウンロードの指示や実行コマンドが含まれています。

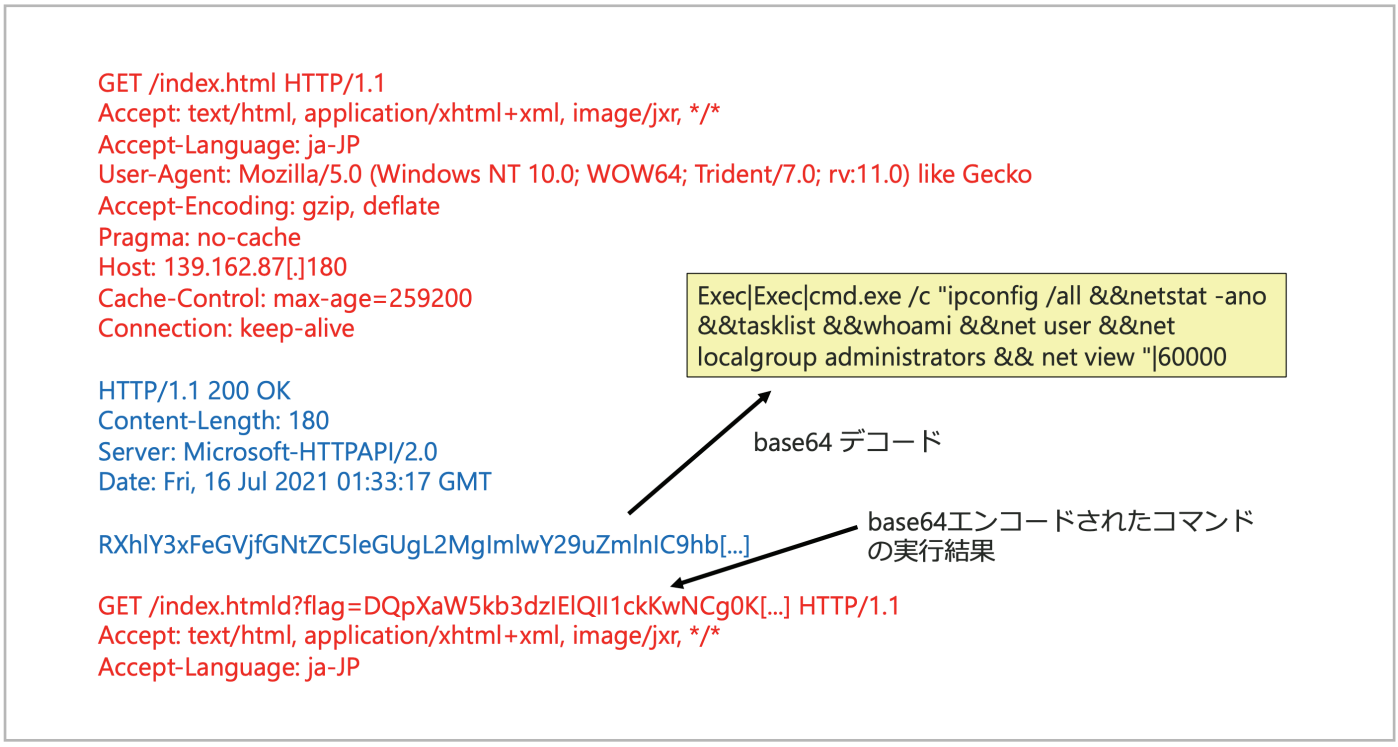


図23. Flagproの通信

10. https://vblocalhost.com/uploads/VB2021-50.pdf
11. https://blogs.jpcert.or.jp/ja/2021/09/gh0sttimes.html
12. https://www.macnica.co.jp/business/security/manufacturers/files/mpressioncss_ta_report_2019_4.pdf

Flagproが情報をサーバにアップロードした場合などに、サーバからは特徴的な文字列”Hello Boy!”を返す特徴がみられました。

```
HTTP/1.1 200 OK
Content-Length: 37
Server: Microsoft-HTTPAPI/2.0
Date: Fri, 16 Jul 2021 02:18:12 GMT

<HTML><BODY> Hello Boy!</BODY></HTML>
```

図24. Flagproが通信する外部サーバからのレスポンス

攻撃者がアップロードされた情報から感染機器が標的であると判断した場合にURLのパス(/robots.txt)を指定し、新たなマルウェアをダウンロードするように指示を出しました。

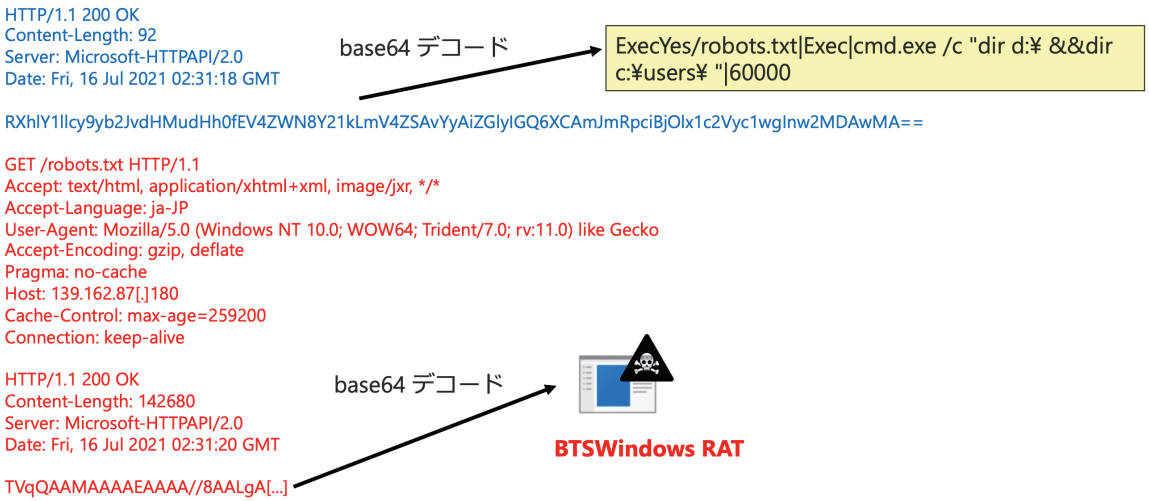


図25. 新たなファイルダウンロードの通信

ダウンロードしたファイルは、サーバからのレスポンスと同様にbase64エンコードされていました。コード分析の結果、このファイルは、BTSWindows RATと呼ばれるバックドアであることが分かりました。

SHA256: 8fe30890f359b8d6e61738265cb5b6d992fc2dc64089d598e8bead3779208887

C2サーバ: www.update.com.live-symantec[.]com

BTSWindows RAT(別名: BTSDoor)

このRATは、2018年に台湾の組織を攻撃するのに使われたのが観測されています。検体に残されていた下記デバッグ情報のパスから"BTSWindows RAT"と呼称しています。C2サーバとは独自プロトコルで通信を行います。

C:¥Users¥Tsai¥Desktop¥20180522windows_tro¥BTSWindows¥Serverx86.pdb
C:¥Users¥Tsai¥Desktop¥20180522windows_tro¥BTSWindows¥Serverx64.pdb

BTSWindows RAT x86
SHA256: ee6ed35568c43fbb5fd510bc863742216bba54146c6ab5f17d9bfd6eacd0f796
ファイル名: ChtIME.exe
C2サーバ: pullnews.postserv.zzux[.]com

BTSWindows RAT x64
SHA256: ae684ffdcd999fd62dcdeb511d0d597a98e0836d57edaa59901da067a7f41576
ファイル名: sesvc.exe
C2サーバ: update.helps.zyns[.]com

Spider RAT

2021年11月にBlackTechのツールの1つであるSpider RATに感染させるオフィスファイルを確認しました。
SHA-256: 0911e5d1ec48430ff9a863f5c4a38f0c71872d8bd6c89f07d6ae16d78eca162f
ファイル名: 2021-10工资中公积金问题咨询.xlsm
C2サーバ: centos.onthewifi[.]com

Spider RATは、HTTPSで外部サーバと通信を行い、リモートからの任意のコマンドとファイルダウンロードなどの操作が可能なRATです。特徴としてはC2への接続、受信命令処理などの主機能毎にスレッドを作成している点です。検体にはデバッグを目的としたメッセージ出力が残されています。

```
v5[76] = 0i64;
v5[76] = beginthreadex(0i64, 0, aa_Work, v5, 0, ThrdAddr);
v6 = *&a1[1].config.data1[4];
if ( *(v6 + 16) )
{
  if ( !sub_1400042A0(v6, 0i64, 1i64, 0i64, 0, 2048, Src) )
  {
    v14 = 15i64;
    v13 = 0i64;
    v12 = 0;
    aa_message(v11, "pWork->HC->HttpSendMessage failed!", 34ui64);
    sub_140002DB0(v11);
  }
  v10 = 0;
  *&a1[1].config.c2[108] = beginthreadex(0i64, 0, aa_handle_c2_command, a1, 0, &v10);
  while ( *(*&a1[1].config.data1[4] + 16i64) )
    Sleep(5000u);
```

図26. Spider RATの検体に残されているデバッグメッセージ

Spider RATが使うUser-Agentは、固定で検体に埋め込まれています。
Mozilla/5.0(Windows NT 6.1; Win64; x64)AppleWebKit/537.36(KHTML, like Gecko)Chrome/88.0.4324.146 Safari/537.36

C2サーバのドメイン centos.onthewifi[.]comと紐づいていたIPアドレス 172.104.109[.]217のレスポンスにFlagproのC2サーバが返すコンテンツ(Hello Boy!)と同一のものが存在し、この点もSpider RATがBlackTechのツールであることを示唆する一つの情報であると考えています。

図27. Spider RAT C2 IPアドレスを持つサーバが過去返したレスポンス内容

他に以下2つの関連検体も見つかっており、これらの検体にはデバッグ情報ファイルのパスが残されていました。この情報からこれらのバックドアを”Spider RAT”と呼称しています。

SHA256: 733b4d5174669caab2bbcc9bfe51606a13346b70af59fccea4f479d1fde7b5d7
Compile Timestamp: 2021-03-19 08:23:25
C2: client.dnsiskinky[.]com

SHA256: d196969b35966462fa03ef857e375e9d6172b34053b115df04cefa3d673b9d85
Compile Timestamp: 2021-03-20 04:56:16
C2: client.dnsiskinky[.]com

・検体に残されていたデバッグ情報ファイルのパス
c:¥users¥amiko¥desktop¥Spider-Rat¥client¥sample1¥x64¥release¥sample1.pdb

また、セキュリティベンダー Blue Hexagonのブログ[13]によれば、Microsoft Exchange Serverの脆弱性 ProxyLogon を悪用した攻撃でSpider RAT
(SHA-256: 733b4d5174669caab2bbcc9bfe51606a13346b70af59fccea4f479d1fde7b5d7)
が見つかっています。このことからBlackTechは、ProxyLogonも標的組織に侵入する手口の一つとして使っていた可能性が高いとみています。

SelfMake Downloader

Spier RATが暗号化されたファイルを外部からダウンロードし、メモリ上で復号・実行するダウンローダを確認しています。その内部に残されていたクラス名の情報から我々は、”SelfMake Downloader”と呼称しています。HTTPユーザエージェントは、固定でファイルに埋め込まれておりSpider RATと同じ文字列が使われていました。
感染経路の一つは、偽装された正規プログラムのインストーラーでの配布です。
SelfMake Loaderをプライバシー保護の高さを売りにしているウェブブラウザ Brave Browserのインストーラーに潜めて感染させるものを確認しています。
SHA256: be5dc0d38251a54350c462a7f4a6c70028ee05c01bde5c1974342893bf12ba5e
ファイル名: Anonymity network tool Setup.msi

ドロップされるSelfMake Downloader
SHA256: 90406d0fc975f342f0e20b49e7946e891392eb06bfc8cc5f3b9b8c86b7c1b17a
ファイル名: browser-up.exe
C2: https[:]//45.77.227[.]248/pfxg.bin

ダウンロードしてくるpfxg.binは、メモリ上で復号されてSpider RAT の32bit版が動作します。

SHA256: c604f7be88bff6fb3d88e53121fb0e247be1e6297eb43cf3bf731c2cdee90594
ファイル名: pfxg.bin

このインストーラーがどのような意図・方法で配布されたかについては特定ができていません。

13. https://bluehexagon.ai/threat-advisory-microsoft-exchange-server/

また、他のSelfMake Downloaderでは下記を確認しています。

SHA256: 1e25116f33f7248e4549cb15fb20bd5d9f87cc7424e6592e565d66095ec2b647
C2: https[:]//exmail.sytes[.]net/pfxg.bin

この検体は、https[:]//exmail.sytes[.]net/pfxg.binをダウンロードし、ファイルをマルチバイトXORでデコードしIAT等を実行できるように修正し、起動します。
セキュリティベンダー Seqrite[14]は、この検体がExchange Serverの脆弱性 ProxyLogonが悪用されて設置されたのを確認しています。

SelftMake Loader

外部サーバからファイルをダウンロードするのでなく、感染機器上に設置されている暗号化されたファイルを探索してロードするローダータイプのものも存在します。

SHA256: 8bdfc1ed5bfec964050a42a0f1ddd8709fcf14fab1ede151c5a7161be904cd96
ファイル名: 不明

SHA256: 92c75df382218e7743359aa83b403e443550e766c8474a59c9dcbd4903a4bf02(ファイルが破損しており実行不可)
ファイル名: 不明

下記場所にあるファイルの先頭4バイトを読み込み、値が0xE0FFD8EEであるかを確認します。
・ローダの実行場所
・C:¥Program Files(x86)¥Common Files
条件に一致したファイルがあった場合、そのファイルを読み込みDownloaderと同じ手順でメモリ上にコードを展開し実行します。

14. https://www.seqrite.com/blog/4898-2/

攻撃グループについて

menuPass(APT10)

menuPass(別称 APT10、Stone Panda)は、米国がAPT10攻撃グループの2名を起訴[15]するまで、日本を標的としてもっとも活発に活動していた攻撃グループです。米国から起訴された後は、大胆で活発な攻撃はなくなりましたが、密かに活動が継続していました。

LODEINFO

2020年初頭から、LODEINFOマルウェアを使った日本を標的とした攻撃が観測されています。これと並行した攻撃が台湾でも観測されており、menuPass攻撃グループの標的とも一致しています。LODEINFOマルウェアを使う攻撃者は、LODEINFOをバージョンアップしながら攻撃を続けるとともに、オープンソースの遠隔操作ツールを使った攻撃を行う事もあります。

A41APT攻撃キャンペーン

過去2年間に渡り、A41APT攻撃キャンペーンでは、SodaMasterなどの独自のマルウェアを使い、主に大企業を標的とした攻撃が観測されています。A41APT攻撃キャンペーンの背後にいる攻撃者は、十分に攻撃リソースがあり非常に洗練されています。SSL-VPN装置の脆弱性を攻撃して標的組織に侵入しますが、SSL-VPN装置へ接続した攻撃者のホスト名の1つ"DESKTOP-A41UVJV"が、この攻撃キャンペーン名の由来です。この攻撃グループは、他の攻撃グループより優れたDLLハイジャックを行い、標的国にC2サーバを設置して攻撃の検出を迂回します。現在、menuPass攻撃グループと強い結びつきを示す新たな調査結果が見つかりつつあります。

BlackTech(HUAPI)

Huapiは、この攻撃グループの攻撃が開始されてからおよそ10年間は主に台湾と台湾に関係の強い国の組織だけを標的として攻撃をしていました。2017年から攻撃範囲を広げ、日本も標的に含まれるようになりました。それ以降、日本と台湾のあらゆる重要な業種を標的として攻撃を行っています。この業種には、政府、軍関連、ハイテク技術、教育、テレコムとメディア関連です。

Huapi攻撃グループのもっとも顕著な攻撃能力は、アンチウィルスや資産管理ソフトウェアの脆弱性を発見してこれを攻撃する事です。例えば、MikroTik(CVE-2021-41987)、Trend Micro(CVE-2021-36741, CVE-2021-36472)、Microsoft Exchangeサーバです。この種の脆弱性攻撃を行えることは、侵入に成功した組織内で、攻撃の水平展開のフェーズで侵害した組織ネットワーク全体を迅速に掌握する事を可能にしています。

15. https://www.fbi.gov/wanted/cyber/apt-10-group

攻撃グループごとのTTPs（戦術、技術、手順）

2021年度に弊社で観測した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。
※この表は、MITRE社 ATT&CK 攻撃フレームワーク version 10[16]に基づき作成しています。

攻撃グループ	攻撃のTTPs	標的組織
APT10 （LODEINFO）	**侵入経路：**スピアフィッシングメール 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 **C2通信の特徴：** 固定の User-Agent（但し Windows10 の正規 Google Chrome と同じ） **ATT&CK：** [Initial Access] Phishing: Spearphishing Attachment（T1566.001） [Execution] User Execution: Malicious File（T1204.002） Officeファイルのマクロを有効にするよう誘導 [Persistence] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder（T1547.001）機器再起動後に自動実行されるようにレジストリ追加 [Defense Evasion] Signed Binary Proxy Execution: Rundll32（T1218.011） 正規ファイルのrundll32を使って悪意のあるDLLファイルのコードを実行 [Defense Evasion] Hijack Execution Flow: DLL Side-Loading（T1574002） 正規ファイルK7SysMon.exeがロードするK7SysMn1.dllをベースにローダを開発 [Command and Control] Application Layer Protocol: Web Protocols （T1071.001）HTTP プロトコル上で暗号化データの通信を行う	メディア、シンクタンク（研究機関）、製造

16. https://attack.mitre.org/versions/v10/

攻撃グループ	攻撃のTTPs	標的組織
APT10 (SodaMaster/ Jackpot)	**侵入経路(エクスプロイト):**SSL-VPN **利用するツール・マルウェア:**SigLoader、SodaMaster、Jackpot **C2通信の特徴:**IPアドレス **ATT&CK:** [Initial Access] External Remote Services(T1133):SSL-VPNの脆弱性または窃取済みアカウントで侵入 [Execution] Command and Scripting Interpreter: PowerShell (T1059.001)イベントログ削除 [Execution] Windows Management Instrumentation(T1047): WMIによるサービスやセキュリティ製品の収集 [Persistence] Scheduled Task/Job: Scheduled Task (T1053.005): スケジューラで常駐 [Persistence] Server Software Component: Web Shell(ID: T1505.003):ウェブシェル様のペイロードで常駐 [Discovery] Software Discovery: Security Software Discovery (T1518.001) [Privilege Escalation] Hijack Execution Flow: DLL Search Order Hijacking(T1574.001):DLLサイドローディング [Defense Evasion] Deobfuscate/Decode Files or information (T1140) [Defense Evasion] Indicator Removal on Host: Clear Windows Event Logs(T1070.001):イベントログの削除 [Credential Access] OS Credential Dumping: Security Account Manager(T1003.002):クリデンシャル窃取 [Credential Access] OS Credential Dumping: NTDS (T1003.003) [Discovery] Account Discovery: Domain Account(T1087.002) [Discovery] Domain Trust Discovery(T1482) [Lateral Movement] Remote Services: RDP(T1021.001) [Collection] Archive Collected Data: Archive via Utility (T1560.001):WinRARによるデータアーカイブ	製造

攻撃グループ	攻撃のTTPs	標的組織
BlackTech	**侵入経路:**スピアフィッシングメール 添付ファイル (Office マクロ)、Exchange Server脆弱性悪用(ProxyLogon)、正規ブラウザインストーラに偽装 **利用するツール・マルウェア:** Flagpro、BTSWindows RAT、Spider RAT、SeffMake Loader **ATT&CK:** [Initial Access] Exploit Public-Facing Application(T1190): ProxyLogonの悪用 [Initial Access] Phishing: Spearphishing Attachment (T1566.001) [Execution] User Execution: Malicious File(T1204.002)Officeファイルのマクロを有効にするよう誘導 [Persistence] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder(T1547.001)機器再起動後に自動実行されるようにスタートアップフォルダにファイルを保存 [Command and Control] Application Layer Protocol: Web Protocols(T1071.001) HTTP/HTTPS プロトコル上で暗号化データの通信を行う	ITサービス

TTPsより考察する脅威の検出と緩和策

マルウェアの配送・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、APT10攻撃グループのLODEINFOマルウェアとBlackTech攻撃グループでは、メールの添付ファイルにマクロのついたOfficeファイルを利用する事が観測されました。2022年4月以降、インターネットから入手したファイルのマクロはブロックされる設定がMicrosoft社のデフォルト[17]になっていくため、マクロファイルでの攻撃テンポは今後低下してくるかもしれません。一方、今後マクロを使った侵入テンポが落ち着けば、他のフォーマットの添付ファイルを使ったスピアフィッシングメールや、深刻な侵入で多く見られるようになったSSL-VPN装置からの侵入に加え、DMZ上にある脆弱なサーバからの侵入が活発になると思われます。本書に該当の攻撃はありませんが、2021年度は、Microsoft Exchangeサーバ、Log4jの脆弱性からの侵入などが、特にセキュリティ担当者がいない海外のグループの会社で目立ちました。これに加え、海外拠点の公開アセットでは、サポート期限切れのOSやミドルウェアが使われていたり、RDP(3389/tcp)などの不用意なポート開放が多数見られます。一定レベル以上のセキュリティ対策がされた本社の公開アセットと比べて、侵入しやすい海外拠点を狙ってくるのは攻撃グループの常套手段になっています。特に海外に多くの拠点を持つ企業においては、一度、全ての拠点における公開アセット(ネットワーク機器やサーバ)を棚卸することをお勧めします。棚卸した中から、対処が必要なものを選別し、暫定対処(撤去、パッチ適用、設定変更)の実施後、必要に応じて脆弱性診断をするという流れです(Attack Surface Management)。

インストールされるRAT、遠隔操作(C2サーバについて)

今回検出されたLODEINFO、A41APT攻撃キャンペーンの検体(SodaMaster、Jackpot)は、正規の実行ファイルとともにロードされるDLLサイドローディングで起動するものでした。サイドローディングで使われたDLLファイルは、DLLファイルのデータセクションなどや別のファイルにある暗号されたペイロードを復号してメモリ上に展開して攻撃を行います。これを検出するため、現在は、ペイロードが動作しているプロセスのメモリを直接スキャンして攻撃を検出し、感染を診断する技術も発達しています。端末の攻撃を検出する手法にForensic State Analysis(FSA)がありますが、メモリのスキャンとペイロードの検出に優れたツールもあり、つぎに述べる導入後の攻撃検出に優れたEDRを使った監視とは違って、現在の状態ですぐに侵害を特定・把握する事ができます。今回観測されたAPT10のA41APT攻撃キャンペーンでは、通信先のC2サーバは感染端末の多くで異なるIPアドレスが観測されており、ネットワークでの検出は難しいものであったと思われます。

17. https://docs.microsoft.com/ja-jp/deployoffice/security/internet-macros-blocked

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や本書で記載したWMIツールなど)を動作させ、遠隔から正規 のコマンドを必ず実行してくる事です。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、C2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。A41APT攻撃キャンペーンは、国内企業の海外拠点からの侵入が多く観測されており、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。

Pyramid of Pain

Pyramid of Painは、David Bianco氏がIOCを分類するために提唱した概念です[18]。攻撃を検出する観点では、このピラミッドの下にいけばいくほど攻撃者が容易に変更しやすく、攻撃の検出を迂回する事ができますが、上にいけばいくほど攻撃者の変更が難しいため、上位にあるTTPsやToolsといった視点で検出のルールを検討しておくことが攻撃の検出に有効であると思われます。たとえば、A41APT攻撃キャンペーンを例にとると、検出されたSigLoaderのハッシュ値は感染端末ごとに異なり、SodaMasterのC2通信先のIPアドレスは同じように検出された感染端末ごとですべて異なっています。すなわち、ハッシュ値やC2のIPアドレスは、たとえ同じ組織であっても検出のインディケータとしてまったく役に立たないと言えます。また、アンチウィルスでの検出率も高くはありません。一方、Host Artifactsに該当するマルウェアが自動起動するためのASEPは、C:¥Windows¥配下の3rdPartyの正規プログラムを使ったサイドローディングでかつスケジュールタスクに設定されるという特徴があり、SigLoaderのセクションで解説したように、この特徴を使ってハンティング検出する事ができます。また、ToolsのPowerShellコマンドを実行する、WinRARでデータを窃取する、Mimikatzでクレデンシャルを窃取するといったToolsの利用も一貫しています。TTPsのクレデンシャルダンプ、マルウェアのASEPをつくる、Windowsの正規コマンドで内部探索するといった攻撃の手口は一貫しており、このピラミッドのより上位に位置するTTPsを検出できるようにする事が有効と思われます。これら上位のTTPs/Tools/Host Artifactの検出は長らくEDRで可能ですが、特にこれらを海外拠点のWindowsサーバに配置しておくと効果が高いと思われます。

18. http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

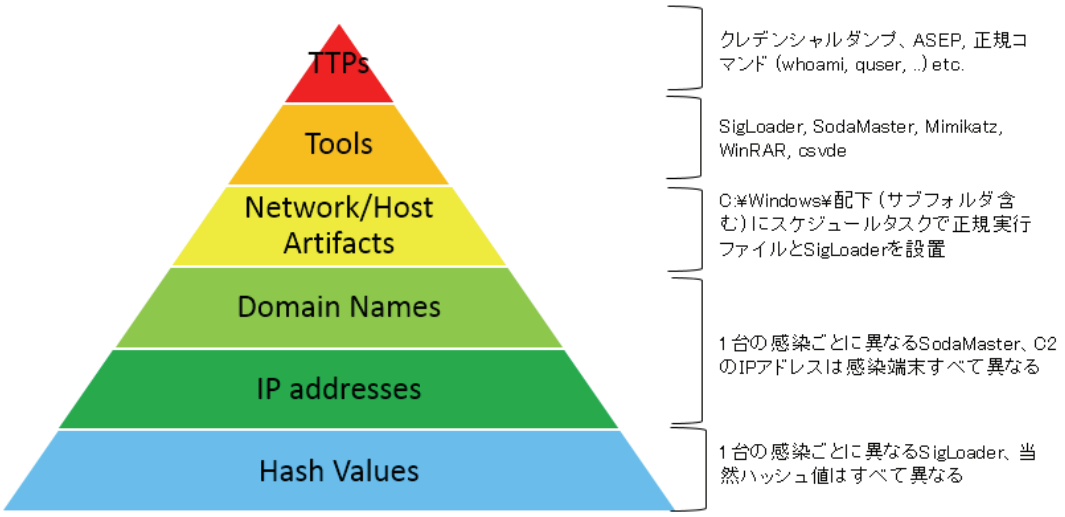


図28. A41APT攻撃キャンペーンとPyramid of Pain

一方で、海外拠点のセキュリティレベル自体をあげて早期に攻撃を検出する必要もあり、推奨対策の提示や、前述のFSAを用いた侵害調査(Compromised Assessment)を一度実施しておき、対策を加速させるはたらきかけも有効だと思われます。

検知のインディケータ

APT10(LODEINFO)

インディケータ	タイプ	備考
f142eecf2defc53a310b3b00ae39ffecc1c345527fdfbfea8ccccd0d69276b41	SHA256	LODEINFO 0.4.9
2169d93f344e3f353444557b9009aef27f1b0a0a8aa3d947b5b8f0b36ef20672	SHA256	LODEINFO 0.5.6
d75537d59954ec3cc092378f00b16b6c9935590ef1074cb308e1ed65e922762c	SHA256	LODEINFO 0.5.6
1dbf67d7dadba5505073aaf3e4478dd295b074bddf10ac5ac7b80d7fc14bea63	SHA256	LODEINFO 0.5.6
fc602ebcf5f9697bedae0e641adfc16985058212f7b9e69dad0f1bf53daf93f9	SHA256	LODEINFO 0.5.6をドロップするドキュメントファイル
http[:]//172.104.78[.]44/	C2	
http[:]//108.61.201[.]135/	C2	
http[:]//139.162.112[.]40/	C2	
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36(KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36 Edg/91.0.86.59	ユーザエージェント	LODEINFO 0.5.6, 0.5.9 固定ユーザエージェント
978ba248c02eb9c130c1459b767527f8a3a9714c6686c12432e027da56f6c553	SHA256	LODEINFO 0.5.9
dab7d79644453a7ca61b9b585c1081167dbe5df0da398df2458c1081295f68e6	SHA256	LODEINFO 0.5.9
50cf6841cbc0ce395a23b9a4d2ddac77b11a376929878717e90c9a7430feddc3	SHA256	LODEINFO 0.5.9
88efbc6e883336a0b910b7bcf0ef5c2172d913371db511a59a4a525811173bf1	SHA256	LODEINFO 0.5.9
e764f26c3e5bf8467da51fbb33c3d80f026b8fe5bd5a6b84318b3f0aedb667cd	SHA256	LODEINFO 0.5.9
88efbc6e883336a0b910b7bcf0ef5c2172d913371db511a59a4a525811173bf1	SHA256	LODEINFO 0.5.9
fde82dcccd471b63f511c6f76dc04e12334818cda8b38f5048b8ad85c9357089	SHA256	LODEINFO 0.5.9をドロップするドキュメントファイル
http[:]//172.105.223[.]216/	C2	
http[:]//45.77.28[.]124/	C2	
https[:]//www[.]dvdsesso[.]com/	C2	

BlackTech

インディケータ	タイプ	備考
ba27ae12e6f3c2c87fd2478072dfa2747d368a507c69cd90b653c9e707254a1d	SHA256	ファイル名:线路信息.xlsm Flagpro をドロップ
e197c583f57e6c560b576278233e3ab050e38aa9424a5d95b172de66f9cfe970	SHA256	Flagpro
http[:]//139.162.87[.]180/index.html	C2	
http[:]//139.162.87[.]180/robots.txt	C2	
8fe30890f359b8d6e61738265cb5b6d992fc2dc64089d598e8bead3779208887	SHA256	BTSWindows RAT
www.update.com.live-symantec[.]com	C2	
ee6ed35568c43fbb5fd510bc863742216bba54146c6ab5f17d9bfd6eacd0f796	SHA256	BTSWindows RAT
pullnews.postserv.zzux[.]com	C2	
ae684ffdcd999fd62dcdeb511d0d597a98e0836d57edaa59901da067a7f41576	SHA256	BTSWindows RAT
update.helps.zyns[.]com	C2	
0911e5d1ec48430ff9a863f5c4a38f0c71872d8bd6c89f07d6ae16d78eca162f	SHA256	ファイル名: 2021-10工资中公积金问题咨询.xlsm Spider RATをドロップ
8c3df0e4d7ff0578d143785342a8033fb6e76ce9f61c2ea14c402f45a76ab118	SHA256	Spider RAT
centos.onthewifi[.]com	C2	
54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b	SHA256	Flagpro
http[:]//org.misecure[.]com/index.html	C2	
c2b23689ca1c57f7b7b0c2fd95bfef326d6a22c15089d35d31119b104978038b	SHA256	Spider RAT ファイル名: DQD964831350012_内容审核权限问题_2021_docx.exe_
42416e73ebc0b776c726e6075fa73bb418f24b53b0b2086141a2aba22301ec6a	SHA256	PLEAD Loader ファイル名: 账号提现问题汇总_20211103_DOCX.EXE
5b2c25873fd873e4cce18afc32b0a2a31ab2c11bed515ef5f671ef5c9fbe86ab	SHA256	ファイル名: 俞通才周报1025-1031.xlsm マクロが破損。マクロを修復し Flagproがドロップされるのを確認
13c19132f7c0c2c02f4070eca9367bdf8ab2bf59c5993c6e853584ac215857c7	SHA256	FrontShell ファイル名: DQ6846846541840O1_运维材料20211028_xlsx.exe
733b4d5174669caab2bbcc9bfe51606a13346b70af5 9fccea4f479d1fde7b5d7	SHA256	Spider RAT
d196969b35966462fa03ef857e375e9d6172b34053b115df04cefa3d673b9d85	SHA256	Spider RAT
client.dnsiskinky[.]com	C2	
1e25116f33f7248e4549cb15fb20bd5d9f87cc7424e6592e565d66095ec2b647	SHA256	SelfMake Downloader

https[:]//exmail.sytes[.]net/pfxg.bin	C2	
be5dc0d38251a54350c462a7f4a6c70028ee05c01bde5c1974342893bf12ba5e	SHA256	偽装Brave Browser インストーラー
90406d0fc975f342f0e20b49e7946e891392eb06bfc8cc5f3b9b8c86b7c1b17a	SHA256	SelfMake Downloader
https[:]//45.77.227[.]248/pfxg.bin	C2	
8bdfc1ed5bfec964050a42a0f1ddd8709fcf14fab1ede151c5a7161be904cd96	SHA256	SelfMake Loader
92c75df382218e7743359aa83b403e443550e766c8474a59c9dcbd4903a4bf02	SHA256	SelfMake Loader 破損しており実行は不可。
dc095fa5f5dca649eaeb7dac01be794938508e01cf417fe881a23dd7467dda3b	SHA256	SelfMake Downloader
manager-server.lflink[.]com	C2	
935e61aba8df5f6e80e001af0fa9c6a50c2cf50f4068e9dd4277f2cd1297d95c	SHA256	SelfMake Downloader
office-service.ftpserver[.]biz	C2	
1d956f5e1e051b58752ab88ce30fbbc229f4f466e7c410f433a386ac21619d74	SHA256	SelfMake Downloader
45.117.102[.]197	C2	
zdx.mefound[.]com	C2	

マクニカは、1972 年の設立以来、最先端の半導体、電子デバイス、ネットワーク、サイバーセキュリティ商品に技術的付加価値を加えて提供してきました。従来からの強みであるグローバルにおける最先端テクノロジーのソーシング力と技術企画力をベースに、AI/IoT、自動運転、ロボットなどの分野で新たなビジネスを展開しています。
その中でセキュリティにおいては、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 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.

株式会社マクニカ

本社　〒222-8561 横浜市港北区新横浜1-6-3 マクニカ第1ビル
〒222-8563 横浜市港北区新横浜1-5-5 マクニカ第2ビル
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6版