www.pwc.com/jp

Operation Cloud Hopper
（クラウドホッパー作戦）

世界規模で被害を出した、前例のないネット上の組織的ハッキング活動を公開する

BAE SYSTEMS
INSPIRED WORK

pwc

目次

はじめに

本報告書は、高い技術力を持つ攻撃者集団が継続的に行ったグローバルな攻撃キャンペーンに関してPwC英国とBAE Systemsが行った調査をまとめたものです。攻撃の対象はマネージドITサービスプロバイダーやその顧客組織で、日本の複数の組織も直接標的とされていました。今回確認されたキャンペーンの規模からは、大規模な作戦行動が行われていたことが推測されます。

本報告書は事実に立脚しており、私たちが評価を加えた箇所についてはその旨を明記しています。また、評価の蓋然性に関しては付録Aに明記した用語を使用しました。

PwC英国とBAE Systemsは、この調査が攻撃技法を広く紹介し、被害の予防策や攻撃検知が適切に行われる一助となればと考え、結果を公表しました。また、広義のセキュリティコミュニティ内で、本報告書で取り上げた攻撃技法への理解がさらに深まり、コミュニティ内で新たな調査成果が発表されるといった進展が加速する契機としたいと考えています。

本調査報告の一環として、PwC英国およびBAE Systemsは、認定インシデントレスポンス（CIR）スキームの下で英国立サイバーセキュリティセンター（NCSC）と協力体制をとり、マネージドITサービスプロバイダーや攻撃対象機関などへの告知や連携にあたりました。

本報告書の補足として、技術的な分析を含むAnnexを別途公開します。

エグゼクティブサマリー

2016年秋以降、PwC英国とBAE Systemsは、中国を拠点とするサイバー攻撃グループによる新たなサイバースパイ活動キャンペーンの被害組織を支援してきた。私たちは、この攻撃グループがセキュリティコミュニティの間に広く知られている攻撃グループ「APT10」と同一であると確信する。私たちが「Operation Cloud Hopper（クラウドホッパー作戦）」（以下Cloud Hopper）と呼ぶこのキャンペーンはマネージドITサービスプロバイダーを標的としたもので、APT10は前例のない規模でマネージドITサービスプロバイダーおよびその顧客組織の機微情報や知的財産への潜在的なアクセスを可能にしてきた。多くの日本の組織もまた、同じ攻撃グループから別のキャンペーンによって同時かつ直接的に標的とされてきた。

私たちが確認した重要な発見を以下に詳説する。

APT10は近年、マネージドITサービスプロバイダーに対する継続的キャンペーンを開始。マネージドITサービスプロバイダーネットワークへの攻略によって、マネージドITサービスプロバイダー顧客ネットワークへの広範な不正アクセスも起こった

- 2016年以降、多数のマネージドITサービスプロバイダーが標的となっていたことはほぼ確実である。APT10は遅くとも2014年からこうした活動を展開していた可能性がある。
- マネージドITサービスプロバイダーのインフラは、多数の被害ネットワークによる（データの）抜き取りルートの複雑な網の目の一部として悪用されていた。

APT10は2016年初頭より、新たなカスタムツールを加えるなど、その規模や能力を相当程度拡大させている

- APT10を含む複数の中国攻撃グループがPoison Ivy（亜種を含む）を使用しているとの報告をFireEyeが2013年に発表し、機能や特徴を詳しく紹介して以降、APT10はその不正プログラムの使用を中止した。
- APT10は主に2014年から2016年にかけて、不正プログラムPlugXの機能向上と配備を継続的に行い、同時に指揮統制機能の標準化を図った。
- 私たちは、オープンソースツールだけでなく、機能を向上させたカスタムメイドの不正プログラムへのシフトも観測している。これは、高い確率で洗練化が進んでいることを示している。

APT10の最新キャンペーンで観測されたインフラは、それまでの彼らの活動とリンクしている

- Cloud Hopperのために使用された指揮統制インフラは、大部分がダイナミックDNSドメインであり、攻撃グループの以前の活動と相互に結び付く。攻撃グループによって悪用される多数のダイナミックDNSドメインは、2016年以降に極端に増加し、活動の加速を表している。
- 日本の組織を直接的に標的としていた攻撃で使われていた複数のトップレベルドメインは、Cloud Hopperに関連するダイナミックDNSドメインのネットワークとIPアドレス空間を共有している。

APT10はスパイ活動に焦点を定め、知的財産や他の取扱注意情報を標的とする

- APT10は攻略したマネージドITサービスプロバイダーやそのクライアントのネットワークを悪用して多数の被害者から大量のデータを抜き取り、秘密裏にデータを世界中に移動させてきたことで知られている。
- 私たちが観測した標的に対する抜き取り行為および大量のデータの特質を見ると、2013年以前のAPTキャンペーン時代を思い起こさせる。

PwC英国およびBAE Systemsは、APT10が高い確率で中国に関連する攻撃グループであると評価する

- サイバーセキュリティコミュニティの間では、APT10が中国の攻撃グループであるとの見方が広く受け入れられている。
- 私たちの分析では、APT10に関連する不正プログラムのバイナリのコンパイル時間、ドメイン登録時間、そして主な侵入活動が、中国標準時間（UTC+8）での活動パターンを示唆している。
- 地政学的な緊張に応えて攻撃グループが照準を定める外交機関や政府組織、特定企業などの標的設定が、中国の戦略的利害と緊密に合致している。

中国の攻撃グループAPT10

中国の攻撃グループAPT10

PwC英国およびBAE Systemsは、APT10がスパイ活動および広範な情報収集に焦点を定める、中国に拠点を置く攻撃グループである可能性が高いと評価する。少なくとも2009年から活動しており、初期の標的は米国の軍事産業基盤（DIB）[1]および技術や通信セクターから始まり、世界中の多数の産業セクターにかけて広範に攻略し、最近はマネージドITサービスプロバイダーに焦点を定めている。

APT10という呼称はもともとFireEyeが定めたもので、PwC英国がRedApolloと呼んでいるほか、BAE SystemsがCVNX、CrowdStrikeがStone Pandaと命名している。一般には広くmenuPass Teamと呼ばれている。この攻撃グループは以前、多くのオープンソースの報告書で取り上げられた。特に有名なのがFireEyeによるPoison Ivyファミリー[2]を使った攻撃グループの詳細報告書、そして同様にTrend Micro[3]が発表したEvilGrabの使用状況に関する詳細な報告書が含まれる。

PwC英国およびBAEのスレットインテリジェンスチームによるAPT10の継続的な追跡や調査と同時に、PwC英国のインシデントレスポンスチームは、APT10の攻略に関連する調査を支援してきた。この調査は、APT10の従来の活動からの変化を評価し、結論を出す材料となっている。

APT10の活動の分析結果から、APT10が2016年の大胆な変革を含む過去3年間の人的、業務的リソースの増強による恩恵を得ていると私たちは確信している。また、2016年から2017年にかけてAPT10が展開してきた活動の規模から、ドメイン登録やインフラ管理、不正プログラム開発、標的活動、解析などの業務別にチームを構成していると私たちは評価する。

APT10は、2013年にPoison Ivyを使った直接的な攻撃から撤退し、PlugXを使うための機能強化およびプラットフォーム改革など、同グループにとって最初と思われるツール設備の刷新を行った。これは、FireEyeの2013年の報告書の公表が原因である可能性が高い。

本報告書では、私たちがCloud Hopperと名付けたマネージドITサービスプロバイダーを執拗に標的とする活動、そして複数の日本の組織を標的とする活動を含む、APT10の最新の活動を詳細に報告する。

1 米国防総省と防衛施設などの設計や開発を手掛け、軍の要件に対応する企業群を指す
https://www.dhs.gov/defense-industrial-base-sector
2 https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-poison-ivy.pdf
3 http://blog.trendmicro.com/trendlabs-security-intelligence/evilgrab-malware-family-used-in-targeted-attacks-in-asia/

APT10の活動の時系列分析

分析の一部として、私たちはAPT10およびそのプロファイルを観測した。それにより、APT10が中国の攻撃グループであるとする私たちの評価が裏付けられた。例えば、私たちはAPT10の活動に関するドメイン登録やファイルコンパイルの時間帯にあるパターンを見いだした。攻撃グループが中国標準時間（CST）に一致するUTC+8のタイムゾーンをベースにしていることが示されていると考えて差し支えない。

図1は、2016年中頃以降APT10が登録したことが分かっているトップレベルドメイン名の登録時間帯[4]（UTC）である。数の推移はAPT10の活動増加を表している。

これをUTC+8にマッピングしたのが図2である。2時間の昼休みを含む中国の営業時間の標準枠が見てとれる。

図1：APT10の活動（ドメイン名登録）の時系列分布（UTC）

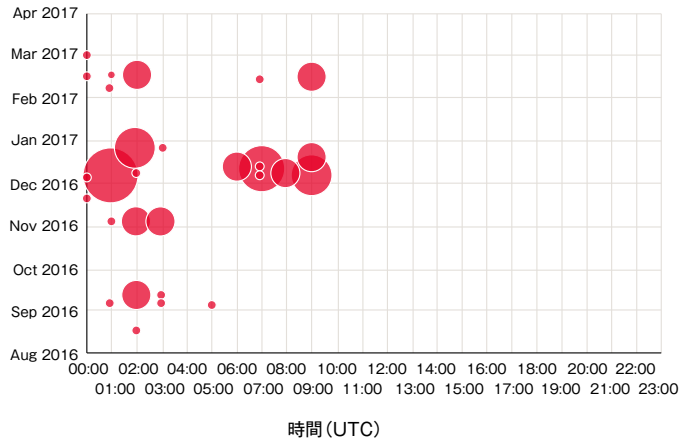
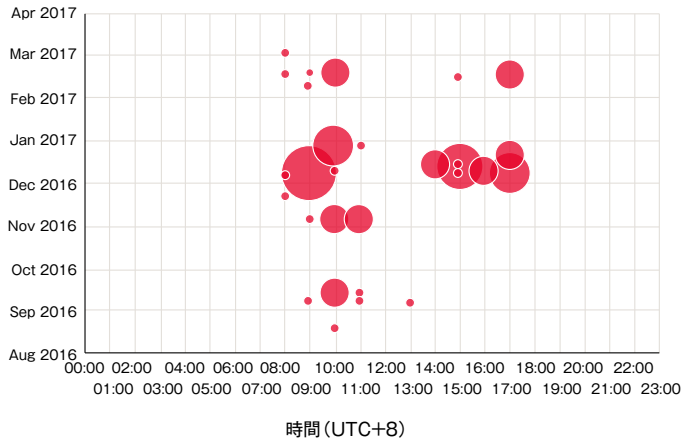


図2：APT10の活動（ドメイン名登録）の時系列分布（UTC+8）



APT10が使うPlugX、RedLeaves、Quasarといった不正プログラムのコンパイル時間帯を分析したところ、図3のように稼働時間帯に同様のパターンが浮かび上がった。

これをUTC+8に当てはめると、ドメイン名登録活動と同様の時間枠が見てとれる。ただし、例えば通常の労働時間外に作業を要求されるなど、この攻撃グループの活動特性と思われる外れ値もある。

図3：PlugX、RedLeaves、Quasarのコンパイル作業時間帯（UTC）

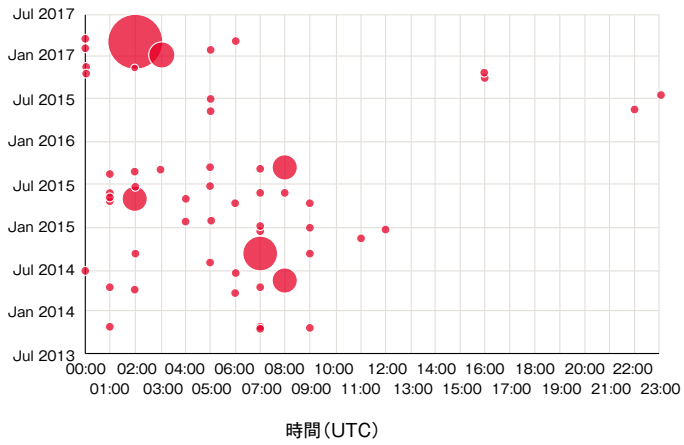
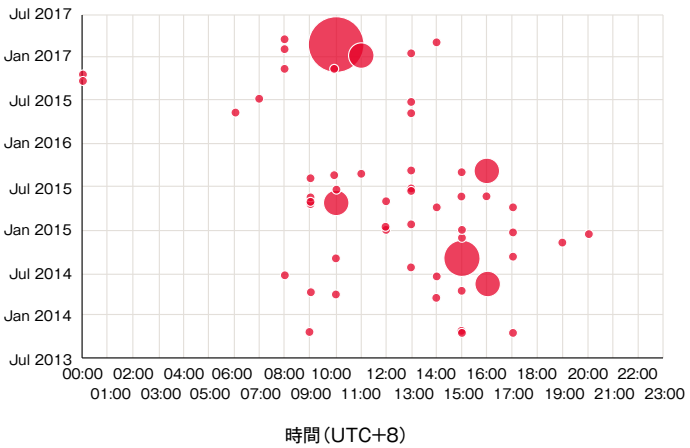


図4：PlugX、RedLeaves、Quasarのコンパイル作業時間帯（UTC+8）



4 図1から図6の中のバブルの大きさはその時点で確認されたイベント数を表す

（最近APT10によって使われる）不正プログラムChChesのコンパイル時間も移行させてみると、図5のように別のパターンが得られる。これは中国の営業時間に合致していないが、目立たないようにするため、かく乱することを目的としてリスク特性を変更した結果か、あるいは開発者によるサイドプロジェクトが最終的に標的活動に使われたことが考えられる。その他の技術的な特徴が重複していることから、ChChesはAPT10だけが使っている可能性が高い。

図5：ChChesのコンパイル時間帯（UTC）

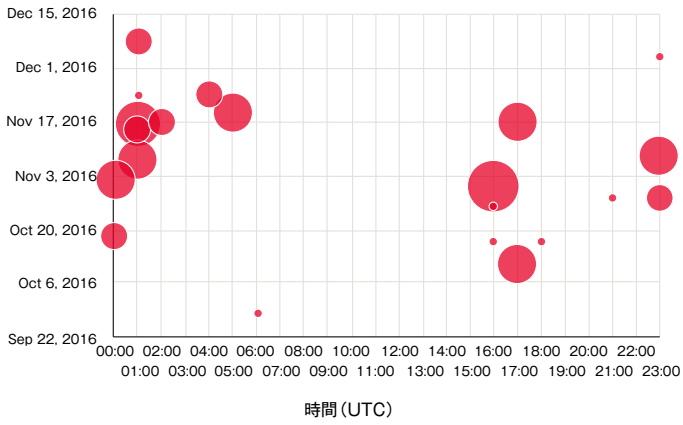
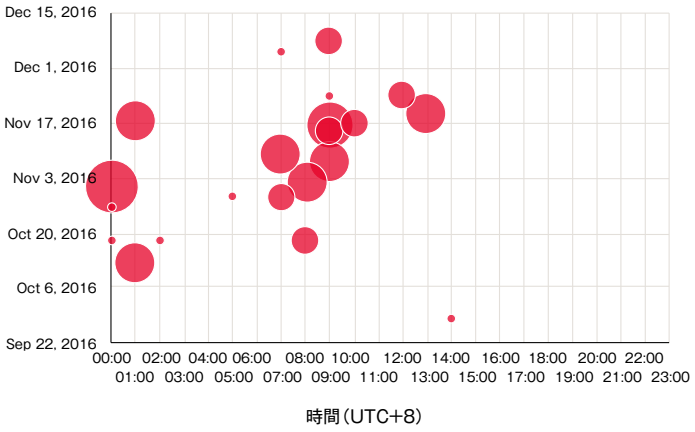


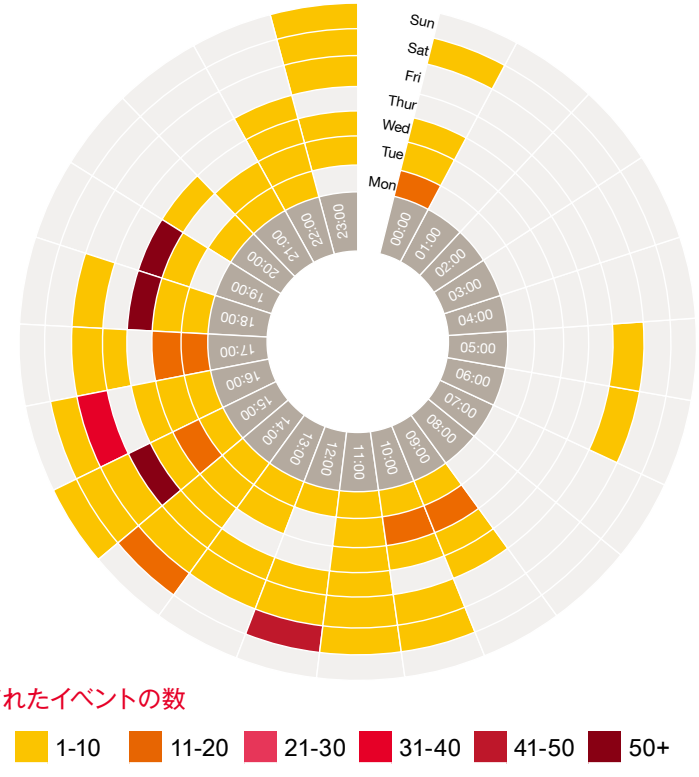
図6：ChChesのコンパイル時間帯（UTC+8）



分析をさらに進めて主に深夜から10：00 UTCの間に発生するAPT10のインタラクティブなやり取りを観測した。これをUTC+8に変換すると（図7）、ここでも中国の営業時間の08：00から19：00までの時間帯へのシフトを見てとれる。図7に見られる週末の作業は、業務上必要になったものと解釈することもできる。

この分析の大意は、米司法省が中国を拠点とする攻撃グループAPT1[5]の関係先とされた複数の個人を起訴した際の証拠とも合致する。それによると、労働日は08：00 UTC+8に開始され、12：00 UTC+8から14：00 UTC+8の2時間の昼休みを経て18：00 UTC+8に終了する。

図7：APT10の活動時間帯（UTC+8）



5 https://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf

APT10 における標的変更の特定

APT10の活動が最初に確認されたのは2009年12月だ。かつては、主に米政府機関や米軍事産業基盤の組織を標的にすることで知られていた。私たちの調査や観測では、この標的設定は今なお続く傾向とみられる。

2013年から2014年にかけて、他の関連するグループと同様、攻撃グループの活動が全般的に下降した。これは、APT1のツールセットやインフラなどの情報が広く出回ったことが原因だとの理解が一般的である。

調査分析から、私たちはAPT10が少なくとも対象を絞った二つのキャンペーンを精力的に行っていたことを明らかにした。キャンペーンはマネージドITサービスプロバイダーとその顧客組織を狙ったものと、直接日本の組織に照準を定めたものだ。

マネージド IT サービスプロバイダーに焦点を定めたキャンペーン

APT10はほぼ間違いなく、いくつかのマネージドITサービスプロバイダーを標的として、前代未聞の規模でグローバルに活動を展開してきた

APT10はマネージドITサービスプロバイダーへの攻撃に助長されて攻撃対象とする産業の幅を広げ、標的設定の範囲と射程を大幅に広げてきた。マネージドITサービスプロバイダーは顧客のITとエンドユーザーのシステムをリモート管理する責任がある。そのため、顧客のネットワークに制約なく直接アクセスできる場合が多い。また、大量の顧客データを社内インフラに保有している可能性もある。

そのため、マネージドITサービスプロバイダーはAPT10のようにスパイ活動に焦点を定める攻撃グループにとっては高い報酬を見込める標的となる。顧客のネットワークに対するマネージドITサービスプロバイダーのアクセスレベルを考慮すると、ひとたびAPT10がマネージドITサービスプロバイダーにアクセスできれば、攻撃を成功させることは比較的容易であり、潜在的には他の組織に攻撃を横展開できる。そうなると、1組織分以上の知的財産や機微情報へのアクセスが可能になる。APT10はマネージドITサービスプロバイダーを介して知的財産を抜き取っていたことが確認されており、従ってローカルネットワークの防護を回避している。

> これ以前に、他の攻撃グループによる同様のサプライチェーン攻撃が観測されていた。例えばオランダ認証局Diginotar（2011年）[6]や米小売業Target（2013年）[7]がその例だ。

APT10がCloud Hopperで使った指揮統制（C2）インフラの大半でダイナミックDNSドメインとの関連性がある。さまざまなドメイン名が共有IPアドレスのホスティングで緊密に相互接続され、さかのぼればAPT10のかなり相当古い時期の活動とも関連性を有する。

現在、APT10の詳細活動の足跡は数千におよび、視覚化は容易ではない。図8は、2016年にAPT10が使用した高水準のインフラ概念図だ。キャンペーンが2017年に入っても継続されているため、攻撃グループが使っている多くのダイナミックDNSドメインが大幅に増加している。

次ページの図9は、図8で示したインフラを抽出し、FireEyeが2014年にブログで公表したAPT10のSiestaキャンペーン[8]当時のインフラに当てはめたものである。タイミングの観点から、インフラの重複を考慮すると、単一の組織がこれら全てのドメインを管理している可能性が高い。

調査を通じて、私たちはAPT10の侵入を受けた多くの被害組織を特定してきた。被害組織のうち複数が、エンタープライズサービスもしくはクラウドホスティングサービスを供給しており、APT10がほぼ間違いなくマネージドITサービスプロバイダーを標的にしているという私たちの評価を裏付けた。私たちは、観測されたマネージドITサービスプロバイダーへの標的は広範囲のサプライチェーン攻撃の一部であると考える。

6 https://security.googleblog.com/2011/08/update-on-attempted-man-in-middle.html
7 https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
8 https://www.fireeye.com/blog/threat-research/2014/03/a-detailed-examination-of-the-siesta-campaign.html

図8：2016年にAPT10が使用していたインフラ概念図

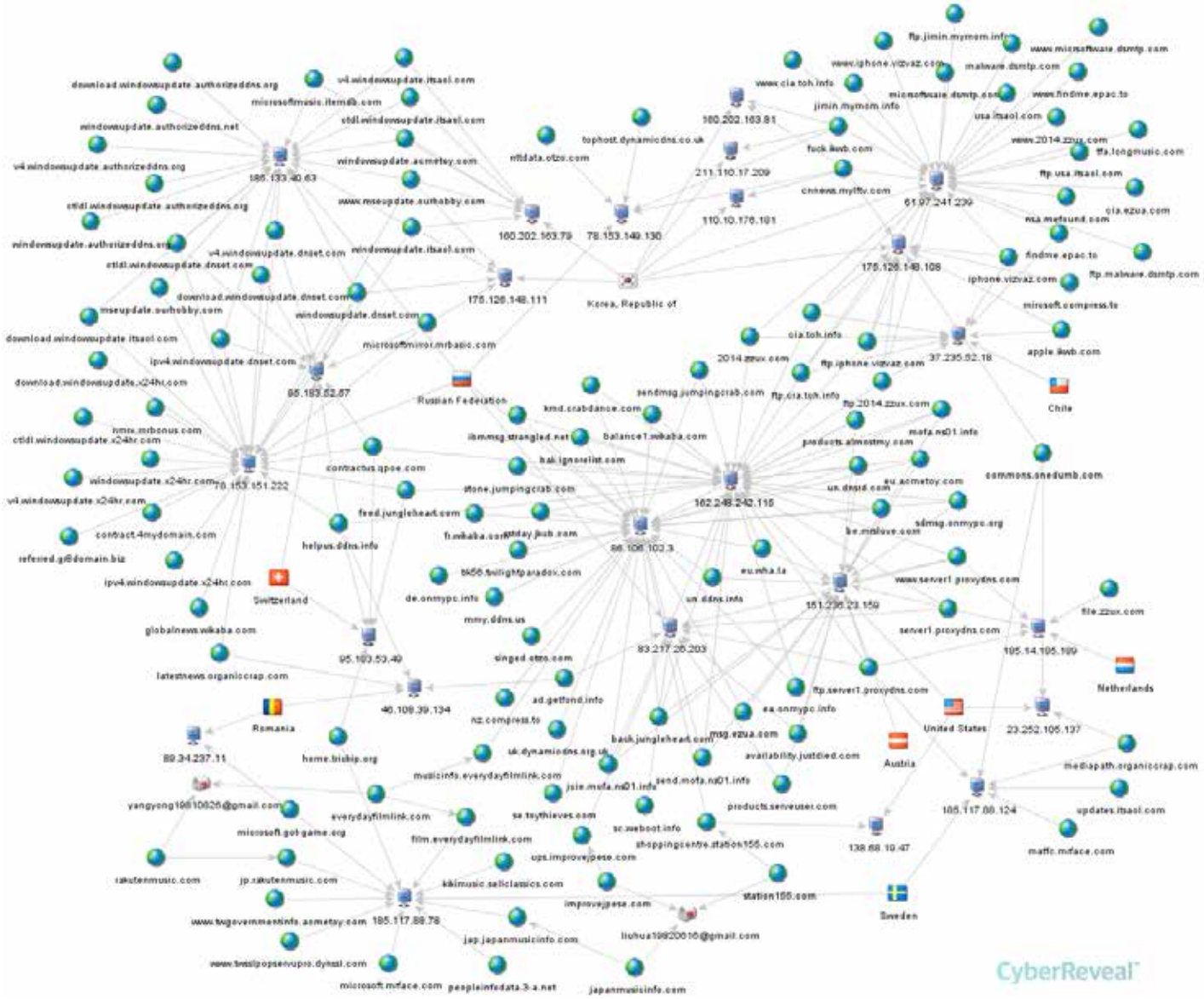
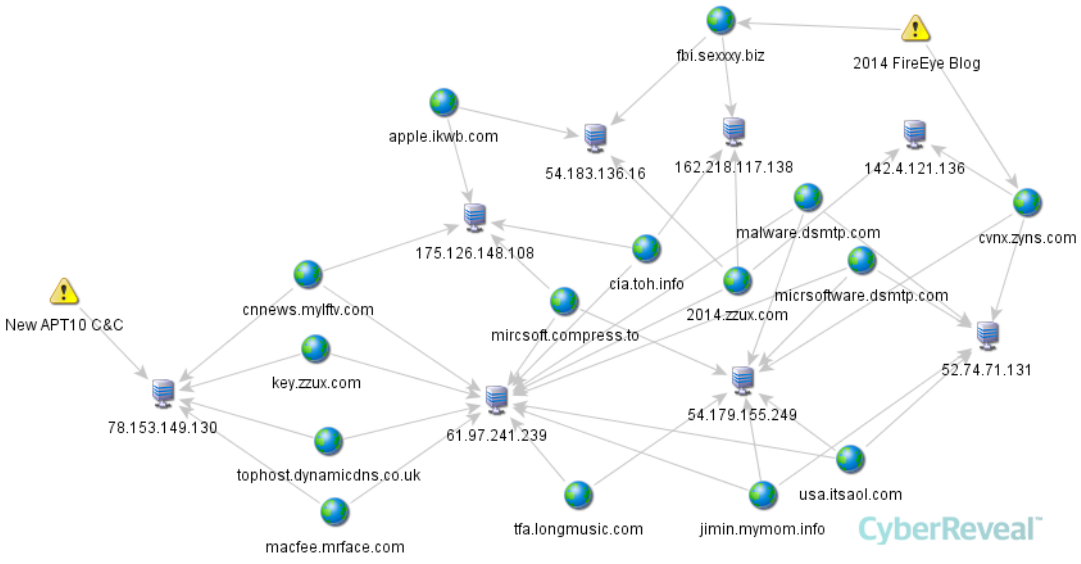
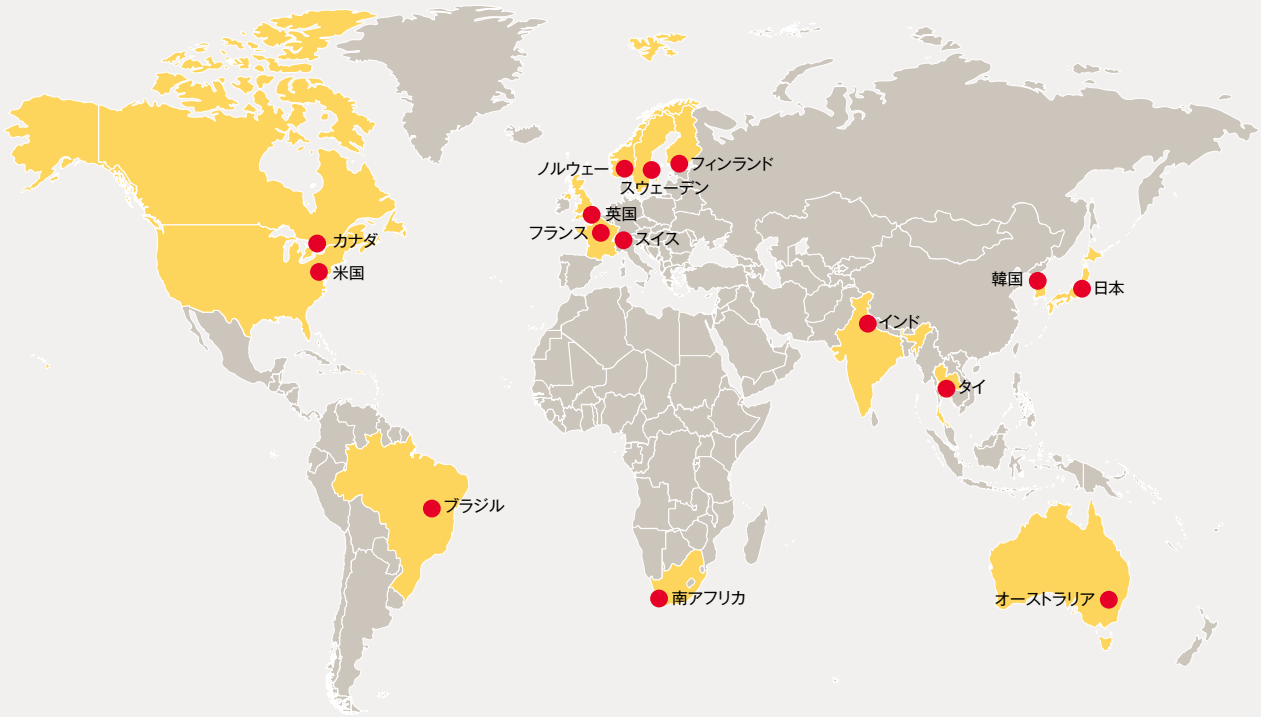


図9：初期のPlugxのドメイン名と最近のAPT10のドメイン名の結び付きを示すインフラ図



標的とされた産業

標的とされた国



日本を狙ったキャンペーン

APT10は、一つの活動区分として一般に「ChChes」と呼ばれるカスタムメイドの不正プログラムを使って体系的に日本の組織を標的にしていた。インフラが共通することからAPT10との関係がうかがわれる一方、活動内容には異なる点があり、グループ内に下部組織がある可能性が示唆される。その活動は、APT10が攻撃対象組織へのアクセスを確立させるために、日本の公的機関（外務省や独立行政法人国際協力機構、自由民主党など）を装っていることが見てとれる。

APT10が日本の組織を標的にしているのは、かつて中国の攻撃グループが日本の広範な産業を標的としたのと同様である。中には、結果として一般企業や政府機関が大量のデータを抜き取られた[9]事例もある。

APT10の標準的な攻撃方法は、いかにも受信者が開きそうな作りの実行ファイルを添付したスピアフィッシングの電子メールを標的に送ることから始まる。特に2016年後半に使われたAPT10の不正プログラムに関連するファイルの最新サンプルを分析すると、日本語のファイル名を使っており、日本語を話す個人を標的としていたことが分かる。ファイルの詳細な分析はAnnex Bを参照されたい。

表1は、このキャンペーンでAPT10が使っていたファイル名の例である。

表1：APT10 が使った日本語名のファイル

ファイル名	訳
1102毎日新聞(回答)._exe	1102 Mainich Newspaper (answer)._exe
2016県立大学シンポジウムA4__1025.exe	2016 Prefectural University Symposium A4_1025.exe
事務連絡案内状(28.11.07).exe	Business contact invitation (28.11.07).exe
個人番号の提供について.exe	Regarding provision of Individual number.exe
日米拡大抑止協議e	Japan-US expansion deterrence conference (e)
ロシア歴史協会の設立と「単一」国史教科書の作成.exe	Foundation of Russian historical association and Composing「a unity」state history textbook.exe

以下に示すのは、三菱重工業の子会社の名をかたる、不正なサイバー攻撃メールの例である。

図10：日本の企業の新製品プレスリリースを基にして作られたおとり文書

深紫外（DUV）レーザーを採用したABLASERの新モデルを世界に先駆け開発ABLASER－DUV、優れた集光性能で超精密加工のさらなる微細化に対応

三菱重工グループの三菱重工工作機械株式会社（社長：白尾 誠二、本社：滋賀県栗東市）は、微細レーザー加工機ABLASER（アブレーザー）の新モデルとして、短パルスの深紫外（DUV）レーザーを採用した「ABLASER－DUV」を世界に先駆けて開発しました。DUVレーザーの特性と集光光学系の最適設計により、長い焦点深度※1を保ったまま集光径を小さくでき、各種穴あけをはじめとする超精密加工もより微細かつ高精度に行うことができます。

ABLASERはレーザー加工機事業の製品第一弾として、2014年度から販売しているもので、高いピーク出力で加工部分をアブレーション（Ablation：蒸発、昇華）させることで、加工面への熱影響を抑えることができ、穴あけ加工では放電加工や従来のレーザー加工を上回る寸法精度と表面の平滑性を確保できます。円錐状穴や鼓状穴といった難しい加工も可能で、一般的な切削加工では困難な高硬度材料や脆性材料の微細高精度加工に貢献しています。

9 http://thediplomat.com/2016/04/japans-achilles-heel-cybersecurity/

APT10の一部組織では、実在する日本の組織の名称に極めて類似したC2用のドメイン名を用意することが知られている。表2は、登録された偽装用ドメイン名と登録項目にあるメールアドレス、偽称されたドメイン名を整理したものである。

表2：APT10 による偽装が確認されているドメイン名

ドメイン名	偽装対象	分野	説明
bdoncloud[.]com	不明	クラウド	汎用的クラウドサービス
cloud-kingl[.]com			
cloud-maste[.]com			
incloud-go[.]com			
incloud-obert[.]com			
catholicmmb[.]com	cmmb.org	宗教	Catholic Medical Mission Board
ccfchrist[.]com	ccf.org.ph		Christ's Commission Fellowship – based in Philippines
cwiinatonal[.]com	cwi.org.uk		Christian Witnesses to Israel
usffunicef[.]com	unicefusa.org	慈善活動	United States Fund For Unicef
salvaiona[.]com	salvationarmy.org		The Salvation Army
meiji-ac-jp[.]com	meiji.ac.jp	国内学術機関	明治大学
u-tokyo-ac-jp[.]com	u-tokyo.ac.jp		東京大学
jica-go-jp[.]bike	jica.go.jp	国内公共機関など	国際協力機構
jica-go-jp[.]biz	jica.go.jp		国際協力機構
jimin-jp[.]biz	jimin.jp		自由民主党
mofa-go-jp[.]com	mofa.go.jp		外務省

今回の攻撃キャンペーンで確認されたC2用のトップレベルドメイン名から、攻撃者とつながりのあるノード特定の材料が得られる。表3にドメイン名登録情報を示す。

表3：一つのネームサーバーを参照する APT10 の登録情報

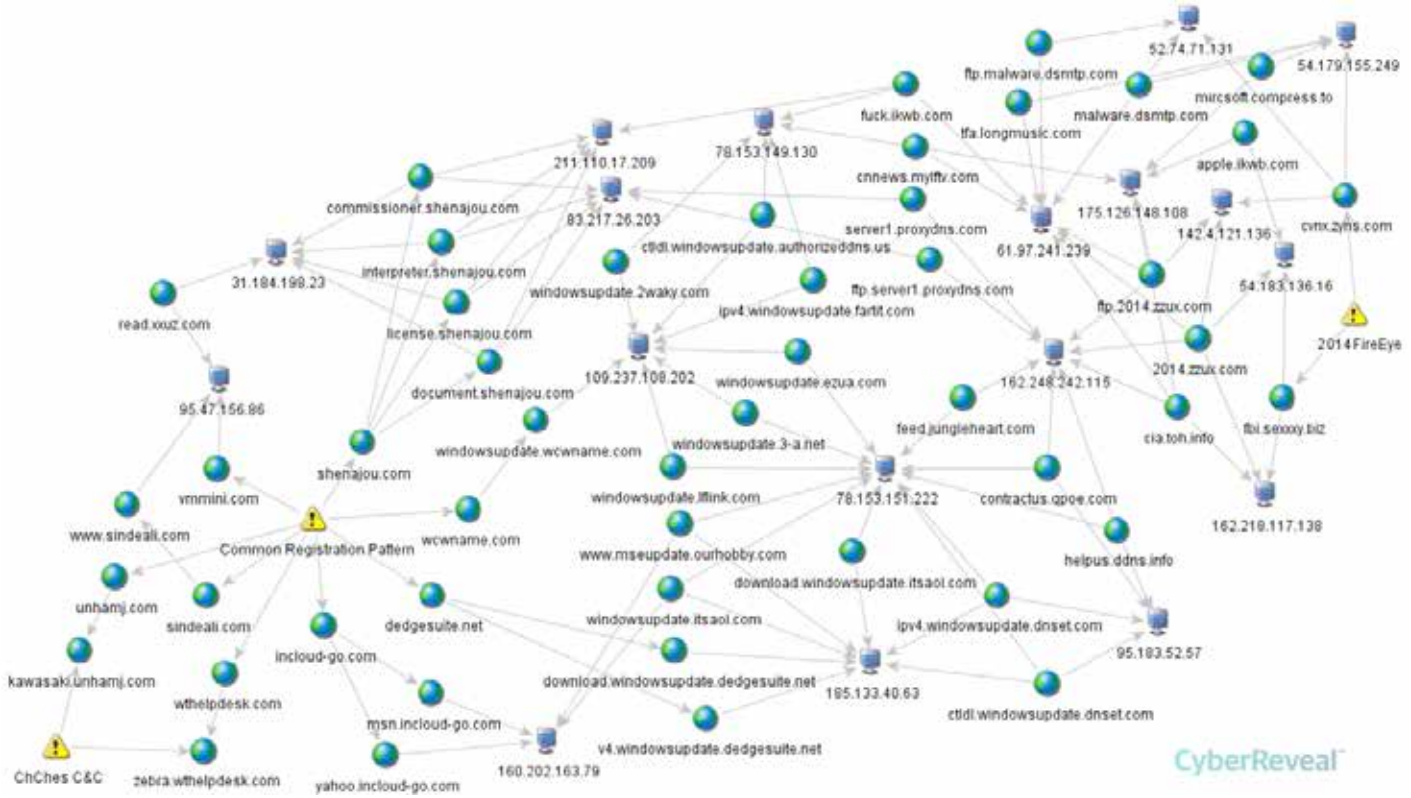
ドメイン名	登録者メールアドレス	ネームサーバー	連絡担当者	連絡担当者所在地
belowto[.]com	robertorivera@india.com	ns1.ititch.com	Roberto Rivera	904 Peck Street Manchester, NH 03103
ccfchrist[.]com	wenonatmcmurray@india.com	ns1.ititch.com	Wenona McMurray	824 Ocala Street Winter Park, FL 32789
cloud-maste[.]com	meganfdelgado@india.com	ns1.ititch.com	Megan Delgado	3328 Sigley Road Burlingame, KS 66413
poulsenv[.]com	abellonav.poulsen@yandex.com	ns1.ititch.com	Abellona Poulsen	2187 Findley Avenue Carrington, ND 58421
unhamj[.]com	juanitardunham@india.com	ns1.ititch.com	Juanita Dunham	745 Melody Lane Richmond, VA 23219
wthelpdesk[.]com	armandovalcala@india.com	ns1.ititch.com	Armando Alcala	608 Irish Lane Madison, WI 53718

登録者が米国所在と記されている以外、連絡担当者情報を共有しているドメインは全くない。連絡先の住所、企業名、氏名は全てドメイン名ごとに異なる。

DNS名前解決のあるドメイン名には、前述のCloud Hopperに関連するダイナミックDNSドメインのネットワークと共通のIPアドレス空間を使用するものもある。

この接続関係を図11の示したインフラ図に示した。複数のChChesのC2ドメインが左下にあり、右端には過去に報告された古いAPT10ドメインがある。

図11：PlugX で使われていたドメイン名と最近の ChChes に関連するドメイン名のインフラ連関図

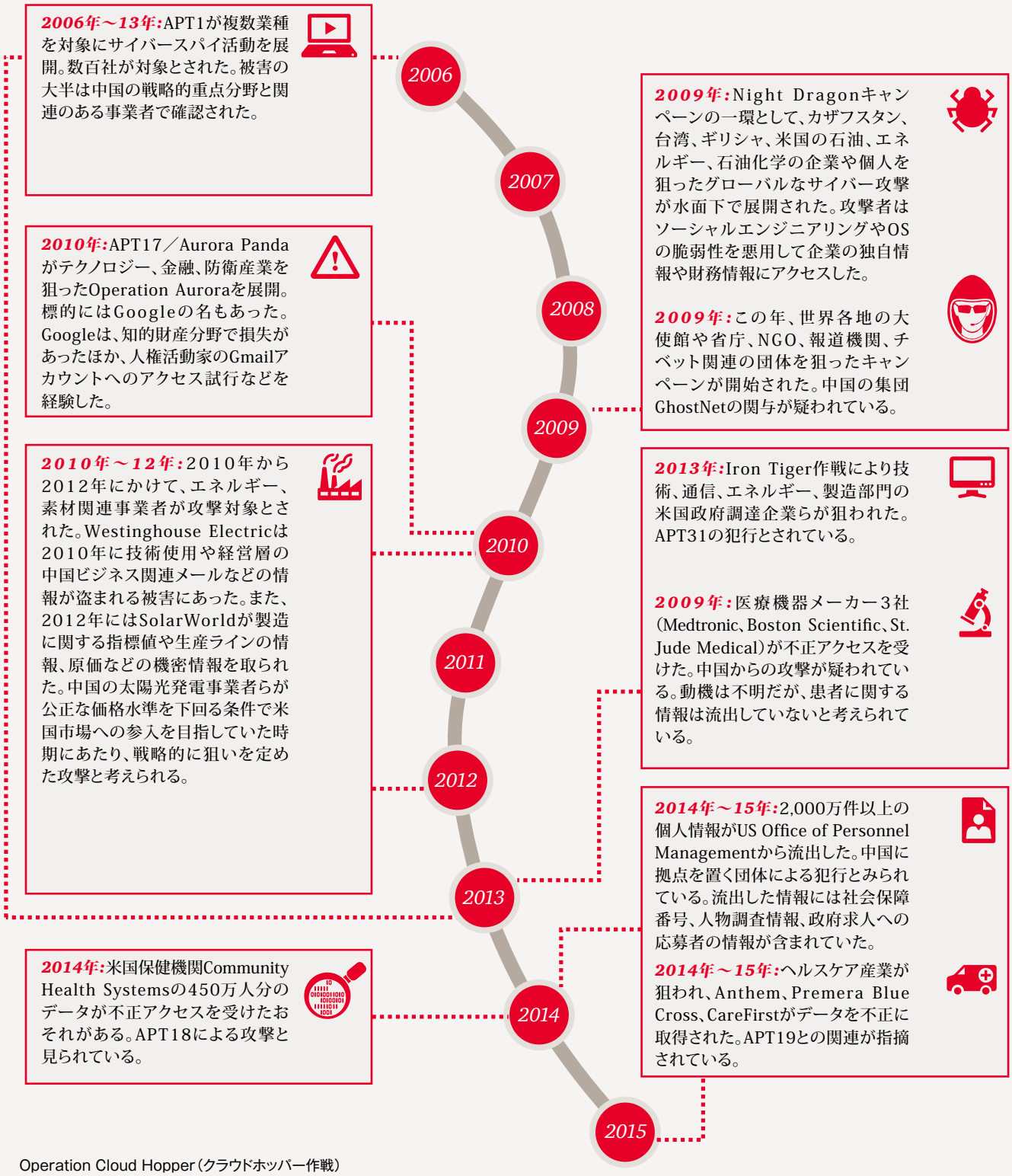


APT10の標的設定の背景

中国から行われたハッキングの小史

中国に拠点を有する攻撃グループは、伝統的な政治、軍事、防衛分野におけるサイバースパイ活動、そして経済的利益のための産業スパイを以前から行ってきた。過去10年で広く知られている事象を以下に示す。

図12：中国から行われたハッキング活動



過去の中国のハッキングとAPT10に共通する傾向

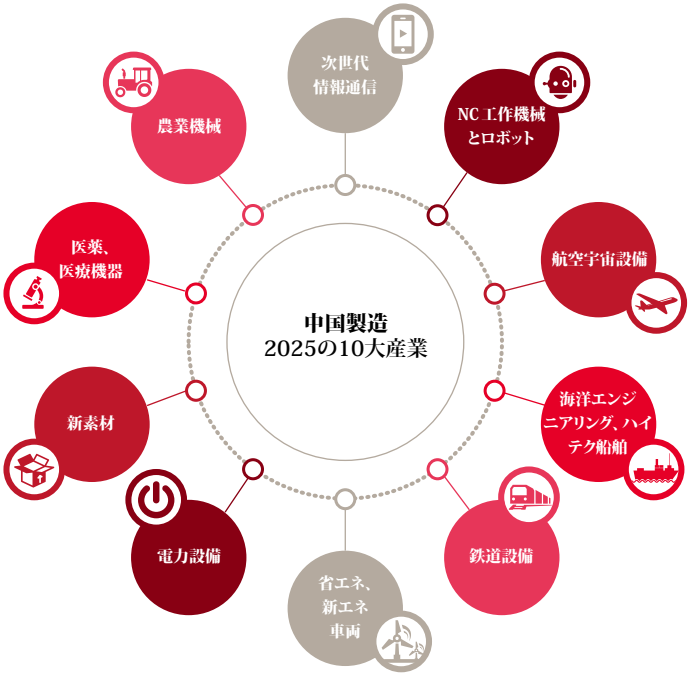
前述の攻撃グループに関連するスパイ攻撃は、中国の経済活動にとって戦略的価値のある組織や、攻撃すれば国内の成長や進歩を促進させることができる知的財産を入手できる組織がこれまで標的とされてきた。

中国に拠点を有する攻撃グループによるとみられる情報収集活動と、中国の五カ年計画に示された戦略的新興産業が合致していると指摘する公開の報告書がある[10]。第13次五カ年計画要綱が2016年3月に採択されたが、APT10の標的とされたセクターや組織が同計画の戦略的目的と広範囲に合致している。五カ年計画で示される目標は、中国の産業発展の方向を定め、同時に中国企業の事業戦略を形成する性質を持つ。

最新の五カ年計画では、2020年までにGDPを2010年水準比2倍にするという中国の目標に沿った五つの発展理念が示されている。発展理念の主軸はイノベーション（創新）、特に技術革新であり、GDPの2.5％に相当する研究開発投資が見込まれる。これにより技術的優位性を実現し、科学技術発展により経済成長貢献度60％[11]の実現につなげるとみられる。このほか、次世代通信、新エネルギー、新素材、宇宙・航空、バイオ医薬、スマートマニュファクチャリング分野にも投資拡大が見込まれる。

中国は、五カ年計画のイノベーション発展理念に加えて「中国製造2025（Made in China 2025）」[12]の一環として10の重要産業で製造業の水準を引き上げる取り組みを進めている。

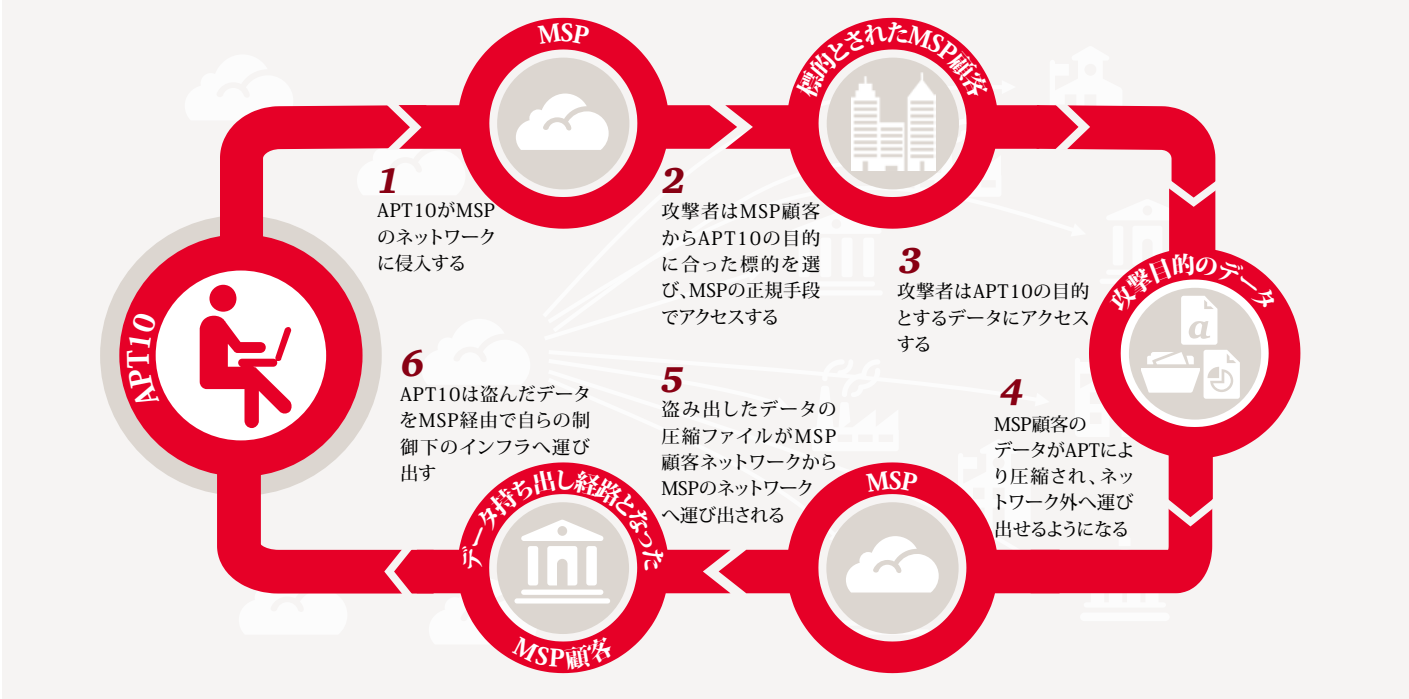
図13：「中国製造2025」で示された10の産業分野



観測されたAPT10の標的は、前述の中国から発したとみられる多くの攻撃の履歴と合致する。それらの標的設定は、中国の第13次五カ年計画と軌を一にしており、中国の目標達成に役立つ情報を有する産業を対象としている。重点産業は多岐にわたり、マネージドITサービスプロバイダーを攻略すると情報収集を進めやすくなる。この戦略では同時に、データを抜き取ったあとに最初に攻略した企業のシステムを経由して元に戻して、解読や追跡をさらに困難にしている。

10 https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
11 https://www.pwccn.com/en/migration/pdf/govt-work-review-mar2016.pdf（https://www.pwc.com/jp/ja/japan-knowledge/archive/assets/pdf/china-13th-5year-plan1604.pdf）
12 http://www.pwccn.com/en/migration/pdf/prosperity-masses-2020.pdf

APT10の手法に着目する



ここでは、APT10の使ったツールと技法、手順（TTP）を詳しく述べる。Poison IvyからPlugXに移行した2014年以降を対象とする。これらのTTPは私たちのインシデントレスポンスおよびスレットインテリジェンス調査の一環として特定され、私たちが直面した最近の二つのキャンペーンでも使われてきた。ここで取り上げる例は、両キャンペーンから抽出されている。

偵察と標的設定

攻撃グループによるペネトレーションの初期段階では、活動が見えないところで行われる傾向があるため、往々にして察知することが困難である。ペイロードを送り込む最も基本的な手法であるスピアフィッシングキャンペーンでAPT10が使用した最新のおとり文書を分析したところ、攻撃グループが標的に対して高水準の調査を行っていることが示唆された。APT攻撃者が通常用いる方法と同じく、APT10は受信者の興味分野に合わせておとり文書を用意している。

図14に示した例において、日本学術振興会のウェブサイトに掲載されている正式文書が“兵器化”され、日本の教育機関へのスピアフィッシングキャンペーンで展開された。

図14：日本の教育機関にAPT10が送り付けたおとり文書

APT10のとる手法として、企業の電子メールアドレスを入手するために偵察段階で調査し、メッセージに不正な添付ファイルか不正なサイトへのリンクURLを仕込むことが知られている。

図15：APT10に関する事象

同じキャンペーンの一環として、私たちは明治大学[14]や中央大学[15]を含む日本の教育機関の多数を標的とした科学研究助成プログラムに関するAPT10[13]の電子メールを観測した。電子メールには、APT10のサーバーからChuChes Powersploit攻撃プログラム（Annex B参照）をダウンロードするリンクのあるZIPファイルが含まれる。

初期攻略と横展開

標的のネットワークに入ったら、攻撃者はすぐさま不正プログラムを設置して足場を築く。継続的に被害ネットワークに接続できるシステムを作ることもある。さらに上位の権限やアクセスを得るために、一般的に使われるようなWindowsツールや、攻略段階の後半ではオープンソースのペネトレーションツール（Annex B参照）を使ってネットワーク構成を把握するなどの偵察活動を行う。

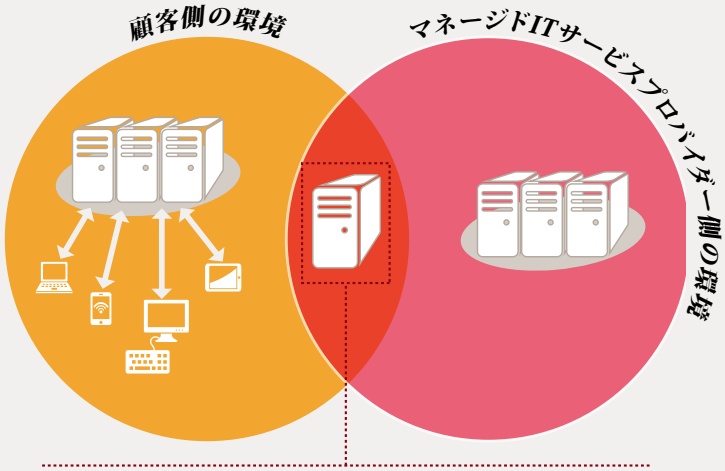
ある事例では、攻撃者は標的ホストがネットに接続されていないと分かるまで、1時間以上をかけてPlugXで外向き通信を確立させようとしていた。接続できないと分かったのち、不正プログラムと全ての関連ファイルは削除された。

APT10は、システムが再起動されても不正プログラムが作動するように、主にタスクスケジュールやWindowsサービスを使って攻撃を持続させている。APT10は、顧客とマネージドITサービスプロバイダーでインフラを共有していることに付け込んで、マネージドITサービスプロバイダー以外の組織へ攻撃を広げる。マネージドITサービスプロバイダー側と顧客側の両方からアクセスできるシステムや、どちらでも有効な認証情報を使ってインフラ間を行き来する。

この偵察行為と並行して、攻撃者は合法な認証情報でアクセスしていることを確認する。APT10がマネージドITサービスプロバイダーを介して標的に侵入した際、マネージドITサービスプロバイダーの認証情報を使い続けていたのを私たちは観測している。さらに高レベルの認証を得るために、APT10は通常、ドメインコントローラに対してmimikatzやPwDumpなどの認証情報窃盗ツール（Annex B参照）を設置する。DLLハイジャックを仕掛けることもある。次に、このレベルのアクセスを維持するために定期的に通信をチェックする。大半の場合、マネージドITサービスプロバイダーの管理者権限もしくはドメイン管理者権限が盗まれる。

アウトバウンド接続を持たない攻略済み環境下のシステムへ攻撃者が不正プログラムをコピーするのが観測されている。

図16：マネージドITサービスプロバイダーと顧客間で共有されるインフラの概念図



顧客側とMSP側にアクセスできる認証情報はAPT10に狙われる。彼らはネットワーク内のアクセス可能範囲を広げるためにこうした認証情報を使う。

13 http://csirt.ninja/?p=1103
14 http://www.meiji.ac.jp/isc/information/2016/6t5h7p00000mjbbr.html
15 http://www.chuo-u.ac.jp/research/rd/grant/news/2017/01/51783/

APT10は、重要度の低いシステムと重要度の高いシステムを同時に狙い、接続を長時間確保しつつ高水準なアクセスを得ようとする。一例として、高価値なドメインコントローラとセキュリティサーバーを攻略する、サポート機能の相対的に重要度の低い、そのためシステム管理者が特段の注意を払うとは考えにくいシステムを特定し、不正プログラムをインストールしてすることが観測されている。

APT10は長期間にわたり被害ネットワークにアクセスする。APT10が攻略したシステムに対して継続的に不正プログラムのインストールやアップデートを行うのが観測された。その大半においてリバースシェルもしくはRDP接続が使われていた。同じやり方でネットワークを越えて組織の規模を拡大させることもある。

Windowsに標準で搭載されているping.exe、net.exe、tcping.exeなどのツールで通信がチェックされることが多い。数秒以内に数台のマシンに対して「net use」コマンドを接続し、5秒程度の短時間で切断する（詳細はAnnex Bを参照）。

ネットワークホッピングとデータ取得

ひとたび被害ネットワークに足場を築けば、APT10は正規のマネージドITサービスプロバイダーやローカルドメインの認証情報、あるいはPlugX、RedLeaves、Quasar RATなどの使い慣れた不正プログラムを使って、目的とするシステムを特定し始める。

攻撃者は、リモートデスクトップ接続かリモートアクセス型トロイの木馬（RAT）でフォルダを確認し、求めているデータの所在を突き止める。見つけたデータは多くの場合「ごみ箱」フォルダにRARやTARのマルチパートアーカイブとして保管され、持ち去られる。圧縮に使うツールは、多くの場合「t.vbs」という名前のリモートコマンド実行スクリプトとして起動される。t.vbsはコマンド出力を攻撃者に返すオープンソースのWMI実行ツールをカスタマイズしたものだ。

アーカイブされたデータが被害組織ネットワークの外に持ち出されたりマネージドITサービスプロバイダーの環境や外部IPアドレスに戻されたりする行動が確認された。その際、下記二つの手順が確認された。また、コマンドラインツールお問い合わせ先t.vbsを使っていた場合もあった。

1. 標的の外部ネットワーク共有を「net use」で開始し、正規のrobocopy ツールでデータを移す
2. 正規のPutty Secure Copy Client（PSCP）（rundll32.exeというファイル名のこともある）を使って第三者のシステムに直接データを転送する

APT10はこうしたやり方で被害ネットワークから他のマネージドITサービスプロバイダーや被害ネットワークなど自分たちがアクセスできるネットワークにデータを「押し出し」、そして同様の方法を使ってデータをそれらネットワークからC2サーバーなど彼らが直接データを得られる場所に「引き出す」。

ネットワーク間をわたって作戦を実行するAPT10の能力は以下のようにまとめられる。

- 正規のマネージド IT サービスプロバイダー認証情報を使って、マネージド IT サービスプロバイダーと複数のマネージド IT サービスプロバイダー顧客のネットワークを結ぶ管理システムに接続する
- リモートデスクトッププロトコルを使ってマネージド IT サービスプロバイダー管理ネットワークとマネージド IT サービスプロバイダー顧客ネットワークのシステムにアクセスする
- t.vbs でコマンドラインツールを実行する
- PSCP と robocopy でデータを転送する

APT10 の不正プログラム

私たちは、APT10の不正プログラムを戦術用と攻撃持続用の二つに分類する。過去のEvilGrabや現在使われているChChes（RedLeavesも同様と考えられる）といった戦術用途の不正プログラムは、動作が軽く、使い捨てで、主にスピアフィッシングで送り込まれる。起動すると、狙いとする重要システムを特定するためにネットワーク内を探索する機能を持つ。他方、過去の例ではPoison IvyやPlugX、現在のQuasarなどの攻撃の持続を目的としたプログラムは、より包括的な機能を有する。これらは重要システムに設置するためのプログラムであり、長期にわたりリモート接続を可能にし、タスクの実行を支援する。

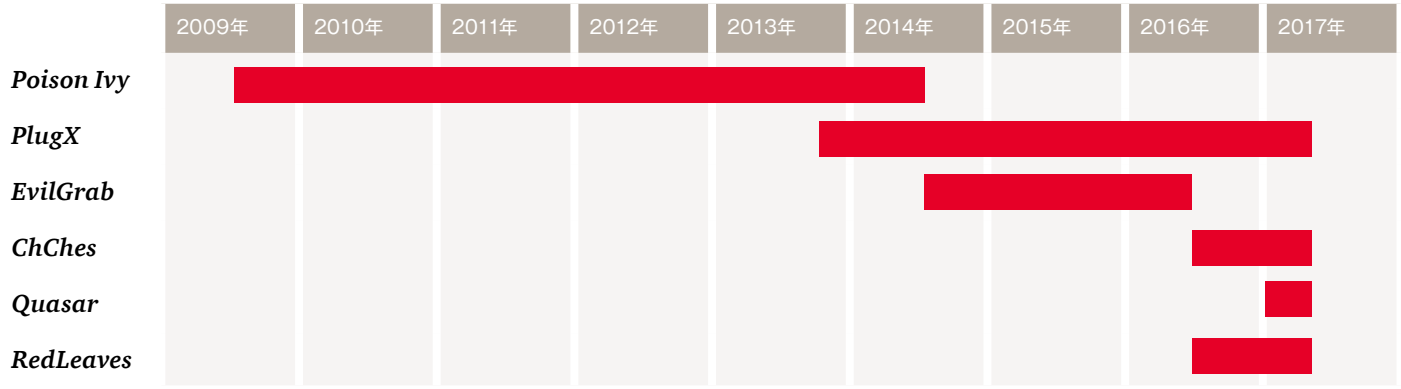
2016年下旬以降、APT10がChChesやRedLeavesなど複数のカスタムメイドの不正プログラムを開発したのが観測された。また、オープンソースの不正プログラムQuasarを取り込み、その機能を拡張し、内部用にバージョンを管理している。

APT10がオープンソースツールの改変版を実行させるためにDLLハイジャックやDLLサイドローディングを使用するのも観測された。PwC英国が観測した事例では、APT10はMimiKatzやPwDump6などのツールからDLLをコンパイルしたり、不正なペイロードをロードするためにWindows Defenderのような署名済みの正規ソフトウェアを使ったりしていた。

Annex Bでは、APT10のツールに対する分析や、攻撃で使われたWindowsツールに関して詳しく分析している。

年表

図17：APT10 の不正プログラム使用の経過



装備刷新の試み

APT10のTTPと並行して、「装備刷新」サイクルも観測された。技術的変化のペースや無料で活用できるオンラインツールやスクリプトの充実により、攻撃グループが自分たちの能力を点検し、多くの選択肢を比較評価していても不思議ではない。私たちは、従来APT10の主力であったツールセットの展開数が減少し、組織内で開発したツールとオープンソースプロジェクトのプログラムの組み合わせが増加したのを目撃している。これはサイバーセキュリティベンダーによる情報公開が影響したためと私たちは確信している。

今回の調査で、私たちは2014年から少なくとも2016年までの期間、多くのPlugX不正プログラムの利用を観測してきた。この傾向とPoison Ivyの利用減少は、大規模な装備刷新が2014年以降に実施されたと考える材料となる。また、PlugXの各バージョンと連携するインフラの詳細分析からも、成熟の過程を看取できる。PlugXの初期バージョンには旧来のドメイン名とIPアドレスがばらばらにかつ明示的に使われていたが最近のバージョンからはドメイン名とIPアドレスの選択に一定の傾向がある。

被害ネットワークを分析する過程で、私たちはAPT10が2016年後半に装備刷新サイクルを再度実行したのを観測した。彼らはQuasar不正プログラム[16]の複数のバージョンを設置してテストしていたほか、カスタムメイドのChChesとRedLeavesを導入していた。

私たちは、PlugXとAPT10を関連付けた報道が頻繁に行われたために簡単に攻撃の出所を推測されるようになり、同じツールを使い続けるわけにはいかなくなった可能性が極めて高いと考えている。

16　https://github.com/quasar/QuasarRAT

結論

APT10は常に進化し続ける高度に持続的な中国の攻撃グループであり、貪欲で大規模な情報収集プログラムを有する。戦略的に標的を定め、広範な産業分野を対象としている。

2013年に活動が露見して以来、APT10はキャンペーンの検知を免れるために何度か大きな変化をとげてきた。PwC英国およびBAE Systemsは産業界や政府と緊密に連携して、私たちが「Operation Cloud Hopper」と呼ぶ他に類を見ないキャンペーンを発見した。このオペレーションはマネージドITサービスプロバイダーに狙いを定め、攻略が成功すればAPT10はその先の多数の組織への足掛かりを得る。日本の組織を標的にしたキャンペーンも観測されている。

APT10は、当初は中国の攻撃グループでは広くみられる不正プログラムを使用していたが、最近のキャンペーンでは独自開発のプログラムを使用しており、確実に進歩している。この傾向はAPT10の精緻化を示しており、ほぼ間違いなく今後も続くと考えられる。APT10の活動が確認された時間帯は中国標準時間（CST）の業務時間帯に合致している。標的設定は他の中国の攻撃グループのものと一致しており、一連のキャンペーンがAPT10による活動であるとする私たちの評価を裏付けている。

このキャンペーンから得られる教訓は、組織がサプライチェーンを含む脅威プロファイルについて包括的な見解を持つことの重要性である。さらに視野を広げると、組織が第三者との関係から生じるリスクを十分に評価し、確認と管理を進めるための適切な手順を踏む必要があることも分かる。

本報告書の補足として、APT10が使用したツールや技法、APT10によるとされる既知の全キャンペーンに関する痕跡情報（Indicators of Compromise）を付録に収録する。これらの情報は、情報提供活動用に英国立サイバーセキュリティセンター（NCSC）に提供されている。

付録

付録A

PwC英国とBAE Systemsの協業について

PwC と BAE Systemsのスレットインテリジェンスチームは、ともに新たなサイバー空間の脅威に対処している。両社はCyber Incident Response（CIR）枠組みの一員として協力関係にあり、情報を共有してAPT10の全貌を把握する取り組みを進めてきた。こうした情報共有は、セキュリティ調査コミュニティの基盤となり、復旧を支援し、セキュリティニーズに沿った企業の意思決定に資する情報を提供する。

蓋然性に関する表記

蓋然性に関する表現は多岐にわたるため、誤読を避けるために本報告書では以下の表現を使用した。評価の確度を示す表現として量的程度を示す際は、下記表記に従った。下記に該当しない場合は統計的分析に基づいた記述である。

表4：評価の確度を示す表記

量的表現	確度の幅
考えにくい	10%~25%
と解釈することもできる	26%~50%
と考えられる	51%~75%
である可能性が高い	76%~90%
と確信している、ほぼ間違いなく~	90%超

付録B

PwC英国による報告書

PwC英国スレットインテリジェンスは、以下のようにAPT10に関する後半な報告書を発行している（一部はサブスクリプションサービスで提供）。

- **APT10 resumes operations with a vengeance**, in Threats Under the Spotlight – CTO-TUS-20170321-01A
- **NetEaseX and the Secret Key to Lisboa** – CTO-TIB-20170313-01A – BlackDLL
- **APT10's. NET Foray** – CTO-TIB-20170301-01B – Quasar
- **APT10 pauses for Chinese New Year**, in Threats Under the Spotlight – CTO-TUS-20170220-01A
- **CVNX's sting in the tail** – CTO-TIB-20170123-01A – ChChes (Scorpion) Malware
- **China and Japan: APT to dispute** -CTO-SIB-20170119- 01A
- **Taiwan Presidential Election: A Case Study on Thematic Targeting**、http://pwc.blogs.com/cyber_security_updates/2016/03/taiwant-election-targetting.html、2016年3月17日発表。EvilGrabの概要、アジア地域、特に2016年台湾総選挙関連を狙った攻撃を取り上げた報告書
- **Scanbox II** – CTO-TIB-20150223-01A
- "IST-Red Apollo-002 – **Red Apollo Tearsheet**"

第三者による報告書

他の機関が著した報告書を以下に示す。

- **RedLeaves – Malware Based on Open Source RAT** - http:/ blog.jpcert.or.jp/2017/04/redleaves---malware-based-on-open-source-rat.html、RedLeavesの技術的側面。オープンソースRATとの関連性を指摘している。
- **The relevance between the attacker group menuPass and malware (Poison Ivy, PlugX, ChChes)**、https://www.lac.co.jp/lacwatch/people/20170223_001224.html、2017年2月23日。APT10と ChChes、Poison Ivy、PlugXの関連性を指摘している。
- **menuPass Returns with New Malware and New Attacks Against Japanese Academics and Organizations**、http://researchcenter.paloaltonetworks.com/2017/02/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/、2017年2月16日発表。APT10による日本の学術機関への攻撃に関して。ChChes やPoison Ivy、PlugX.に関する女王法も収録。
- **ChChes – Malware that Communicates with C&C Servers Using Cookie Headers**, http://blog.jpcert.or.jp/2017/02/chches-malware--93d6.html、2017年2月15日発表。ChChes の情報と攻撃の痕跡を紹介。
- **PlugX TrendMicro "tearsheet"**, https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/plugx、2016年9月7日発表。PlugXの情報と攻撃の痕跡を紹介。
- **A Detailed Examination of the Siesta Campaign**,
- https://www.fireeye.com/blog/threat-research/2014/03/a-detailed-examination-of-the-siesta-campaign.html、2014年3月12日発表。Siestaキャンペーンの詳細が分かる。
- **POISON IVY: Assessing Damage and Extracting Intelligence**, https:/www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-poison-ivy.pdf、2013年8月21日発表。Poison Ivyの技術的情報とmenuPassなどのキャンペーン例。
- **EvilGrab Malware Family Used In Targeted Attacks In Asia**, http://blog.trendmicro.com/trendlabs-security-intelligence/evilgrab-malware-family-used-in-targeted-attacks-in-asia/、2013年9月18日発表。EvilGrabの技術的概観。
- **CrowdCasts Monthly: You Have an Adversary Problem**、https://www.slideshare.net/CrowdStrike/crowd-casts-monthly-you-have-an-adversary-problem、2013年10月16日発表。中国のアクターのAPTや犯罪、ハクティビストの活動に関するプレゼンテーション。Stone Panda（APT10）を一節を割いて紹介。
- **PlugX: New Tool For a Not So New Campaign**, http://blog.trendmicro.com/trendlabs-security-intelligence/plugx-new-tool-for-a-not-so-new-campaign/、2012年9月10日発表。PlugXの概要。
- **Pulling the Plug on PlugX**, https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/112/pulling-the-plug-on-plugx、2012年8月4日発表。PlugXの技術的概観と用途を紹介している。

About PwC

PwC Japanグループでは、クライアントの課題解決のために、監査およびアシュアランス、コンサルティング、ディールアドバイザリー、そして税務、法務において、国内およびグローバルにおける複雑な経済環境で活躍される皆様に、きめ細かなサービスを提供しています。

BAE Systems について

BAE Systemsは、先進のテクノロジディフェンス、宇宙航空、セキュリティに関するソリューションを提供しています。

BAE Systems Applied Intelligenceでは、サイバー犯罪の被害防止やネットワーク接続のリスク低減、規制対応、事業変革で世界中の国家や政府、事業体を支援しています。膨大なデータを収集、分析して独自のソリューションとシステム、経験とプロセスを基にサービスを提供しています。

サイバーセキュリティに関する
ご相談／お問い合わせ先はこちらまで

Mail：JP_Cons_pcs.info@pwc.com

PwCサイバーサービス合同会社
〒104-0061 東京都中央区銀座8-21-1
住友不動産汐留浜離宮ビル
Tel：03-3546-8480
http://www.pwc.com/jp/cybersecurity

www.pwc.com/jp

本報告書は、PwCメンバーファームが2017年4月に発行した『Operation Cloud Hopper』を翻訳したものです。翻訳には正確を期しておりますが、英語版と解釈の相違がある場合は、英語版に依拠してください。
電子版はこちらからダウンロードできます。 www.pwc.com/jp/ja/japan-knowledge/thoughtleadership.html
オリジナル（英語版）はこちらからダウンロードできます。 www.pwc.co.uk/issues/cyber-security-data-privacy/insights/operation-cloud-hopper.html
日本語版発刊年月：2017年6月　　管理番号：I201704-3