Falcon Day vol.4
脅威インテリジェンスとFalconの防御

2018年12月11日

マクニカネットワークス株式会社

勅使河原　猛

インテリジェンスとは？

攻撃者の目的

攻撃者の情報

脆弱性

マルウェアの
ハッシュ

マルウェアの通信先

攻撃手法

インテリジェンスの区分

現在、DoD（米国国防省）では、脅威情報を以下の３つに分類しています。

① 戦略的インテリジェンス – 攻撃者の動機など上層部の判断用

② 運用的インテリジェンス – 脆弱性など日々の意思決定などの判断用

③ 戦術的インテリジェンス - IOCなどのオペレーターの判断用

参考：https://securityintelligence.com/security-intelligence-at-the-strategic-operational-and-tactical-levels/

インテリジェンスとは？

① 戦略的インテリジェンス

- 攻撃者の目的
- 攻撃者の情報

② 運用的インテリジェンス

- 脆弱性
- 攻撃手法

③ 戦術的インテリジェンス

- マルウェアのハッシュ
- マルウェアの通信先

アジェンダ

- 戦略的インテリジェンスの視点
- 戦術的インテリジェンスの視点
- Falcon vs. APT

戦略的インテリジェンス

国家支援のサイバー攻撃者たちの攻撃の背景は？

国家に利益をもたらすため

- 国境問題など外交にまつわる情報収集
- 政策に関連した情報収集
- 外貨獲得の為の攻撃
- **国家産業を発展させるための情報収集**

2018年10月 中国人が米国司法省に起訴

米国司法省によって中国人に対する２つの起訴が発生

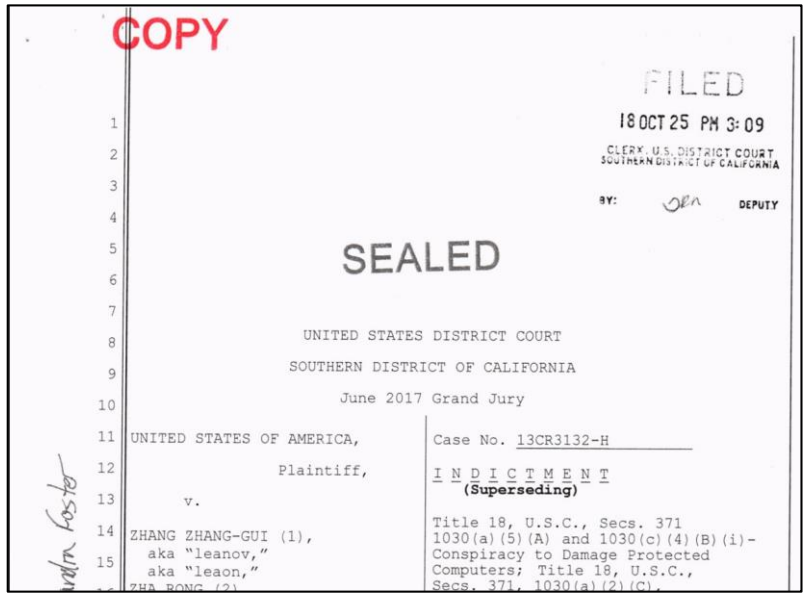
① 10月10日 GEアビエーション社などの**航空宇宙分野の企業**から機密情報の窃取を目的とした産業スパイを実施した疑いで**江蘇省の中国国家安全省**の役人を起訴

② 10月30日 キャプストーン・タービン社を含む欧米の**航空宇宙企業分野**の企業に対するハッキングによるサイバースパイ及び産業スパイによって機密情報を窃取した疑いで**江蘇省の中国国家安全省**の役人を含む10名を起訴

参考① https://jp.reuters.com/article/us-arrest-china-spy-idJPKCN1MK2PL
参考② https://jp.reuters.com/article/usa-china-cyber-attack-idJPKCN1N502J

起訴状から読み解く攻撃者

- “On or before May 24, 2012 a member of the conspiracy installed ***Winnti*** malware in capstone Turbine’s computer systems” (P.11)
- “Malware, including but not limited to certain malware, such as ***Sakula*** and ***IsSpace***, that was uniquely used by members of the conspiracy during the period of the conspiracy,” (P.8)



COPY

FILED
18 OCT 25 PM 3:09
CLERK, U.S. DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA
BY: DEPUTY

SEALED

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

June 2017 Grand Jury

UNITED STATES OF AMERICA,

Plaintiff,

v.

ZHANG ZHANG-GUI (1),
aka “leanov,”
aka “leaon,”

Case No. 13CR3132-H

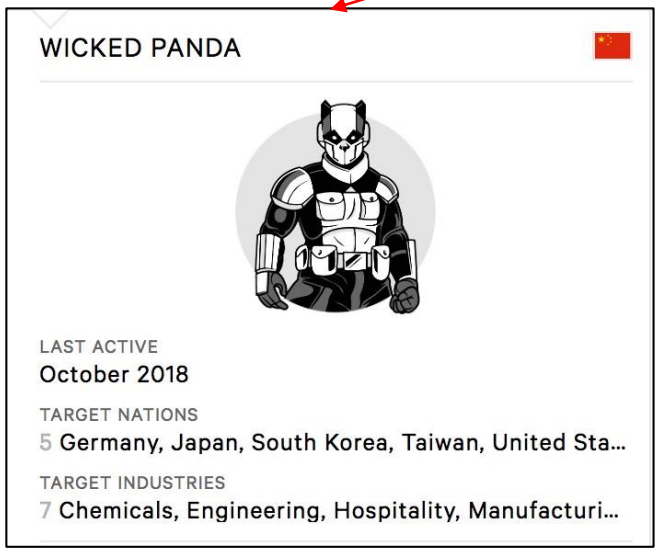
INDICTMENT
(Superseding)

Title 18, U.S.C., Secs. 371 1030(a)(5)(A) and 1030(c)(4)(B)(i)- Conspiracy to Damage Protected Computers; Title 18, U.S.C., Secs. 371, 1030(a)(2)(C),

https://www.justice.gov/opa/press-release/file/1106491/download
http://static.politico.com/e8/1b/7159ae1046d09ee1e59d95aef1f8/indictment-of-yu-pingan-for-providing-malware-used-to-hack-western-companies.pdf

起訴状から読み解く攻撃者（2）

- “On or before May 24, 2012 a member of the conspiracy installed *Winnti* malware in capstone Turbine’s computer systems” (P.11)
- “Malware, including but not limited to certain malware, such as *Sakula* and *IsSpace*, that was uniquely used by members of the conspiracy during the period of the conspiracy,” (P.8)

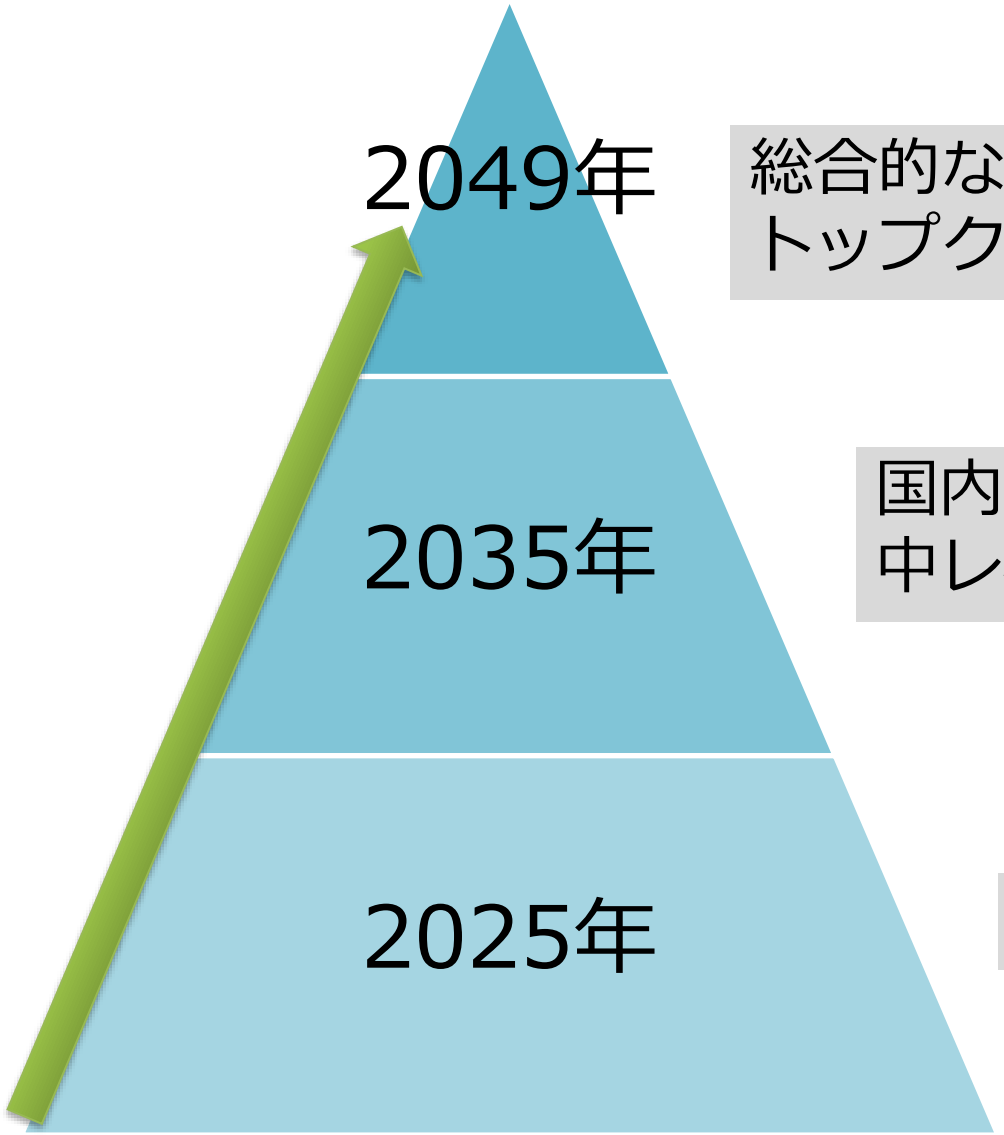


YU PINGAN a.k.a. "GoldSun"

マルウェアの譲渡

https://www.justice.gov/opa/press-release/file/1106491/download
http://static.politico.com/e8/1b/7159ae1046d09ee1e59d95aef1f8/indictment-of-yu-pingan-for-providing-malware-used-to-hack-western-companies.pdf

「中国製造2025」 - 中国の政策の１つ



総合的な実力で世界の製造強国の
トップクラスに入ること

国内製造業の全体水準を世界「製造強国陣営」の
中レベルに引き上げること

製造強国に仲間入りすること

「中国製造2025」の9つの戦略任務と10個の重点産業分野

9つの戦略任務
製造業のイノベーション能力の向上
情報化と工業化の高度な融合の推進
工業の基礎能力の強化
品質とブランドの強化
グリーン（環境保全型）製造の全面的推進
重点分野の飛躍的発展の推進
製造業の構造調整の推進
サービス型製造と生産関連サービス業の推進
製造業の国際化レベルの向上

重点産業分野
次世代技術情報
高度なデジタル制御の工作機械とロボット
航空・宇宙設備
海洋エンジニアリング設備とハイテク船舶
先進的な軌道交通設備
省エネ・新エネ車
電力設備
農業機械
新材料
バイオ医薬・高性能医療機器

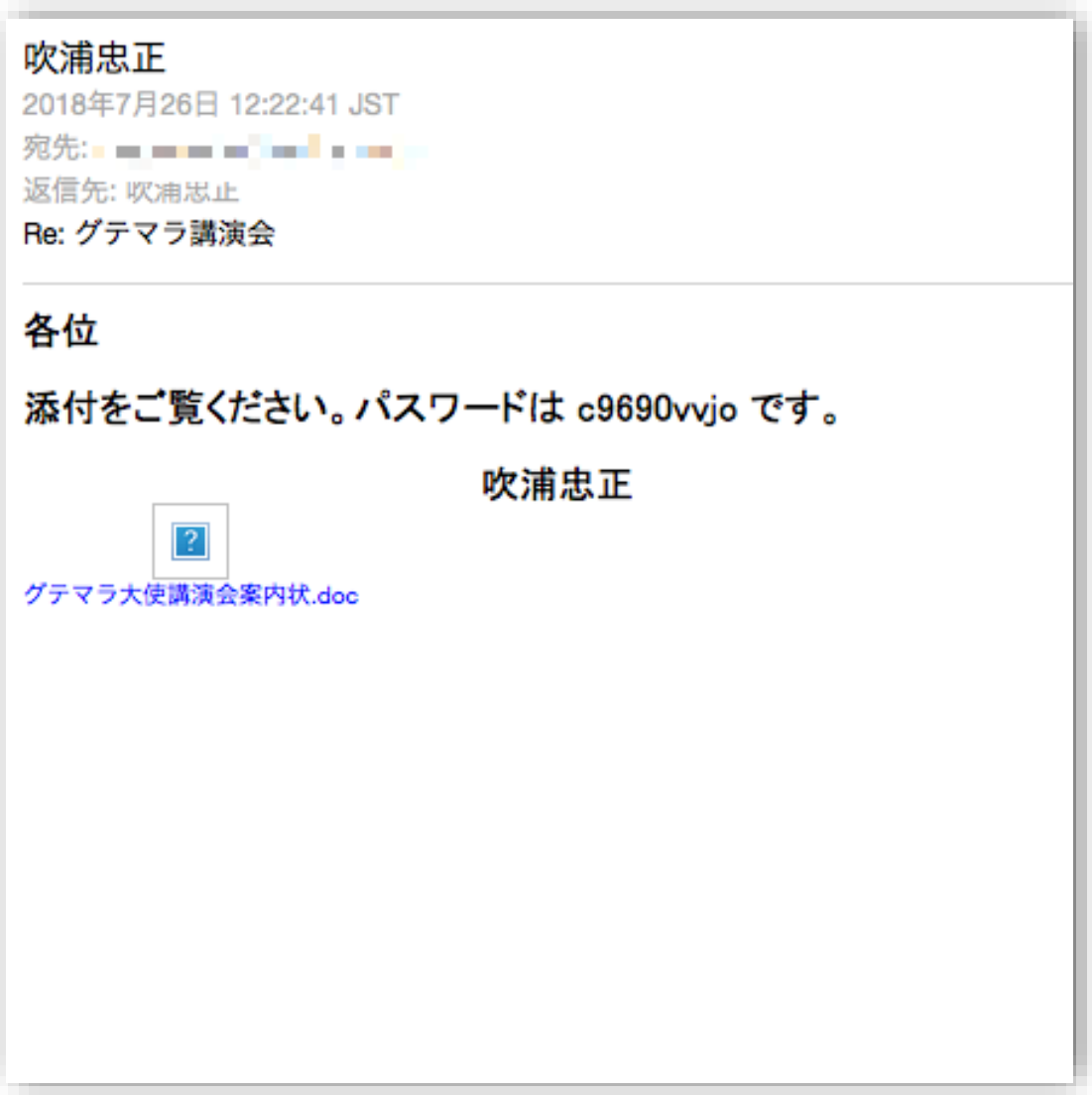
「中国製造2025」- 10個の産業分野

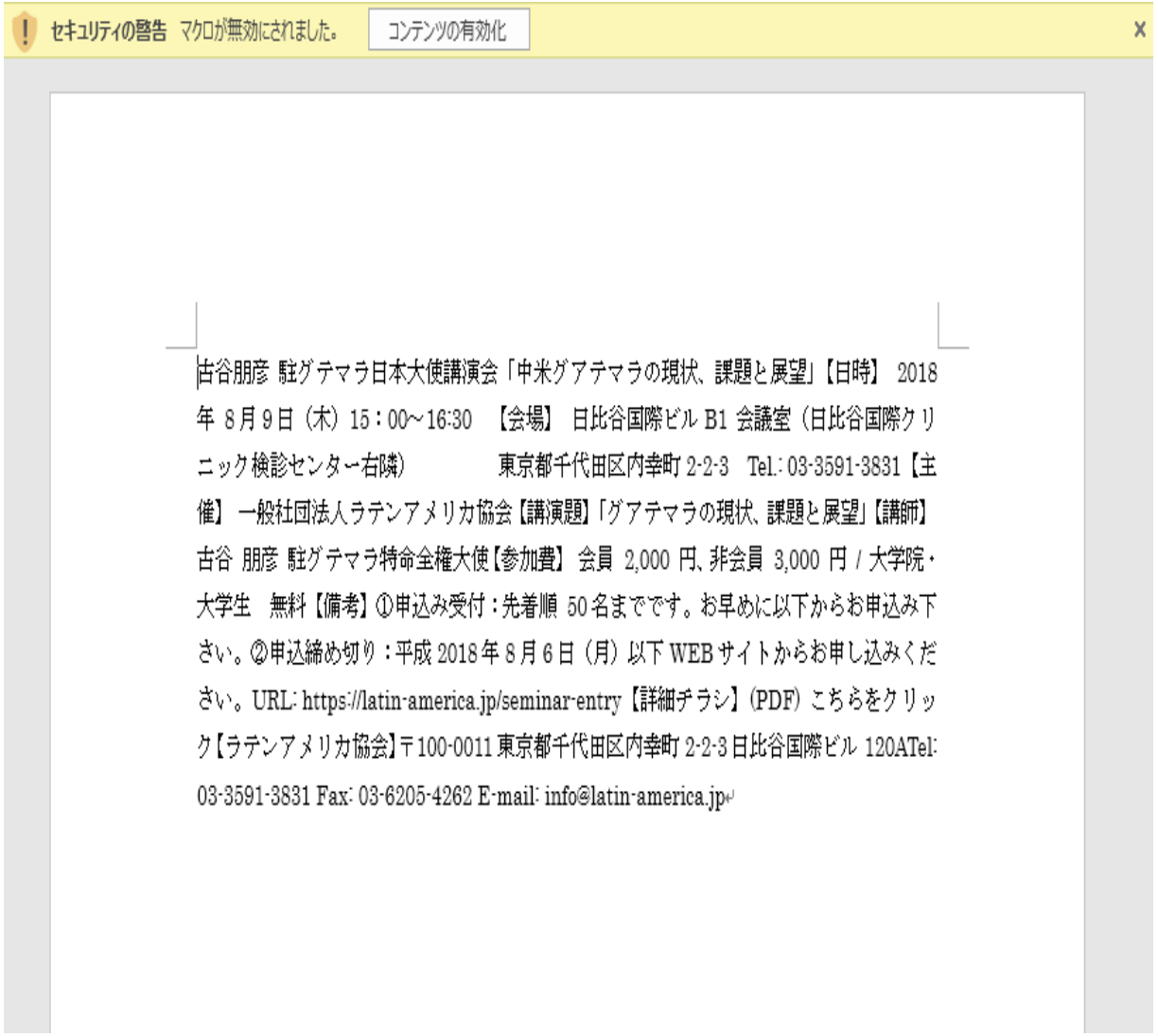
産業分野	主なプロジェクト例
次世代情報技術	集積回路設計、情報通信設備、ネットワークセキュリティ、5G（第5世代モバイル通信技術）
高度なデジタル制御の工作機械とロボット	産業用ロボット、高品位CNC工作機械
航空・宇宙設備	ターボプロップ（シャフト）エンジン、次世代ロケット、宇宙インフラの建設
海洋エンジニアリング設備とハイテク船舶	海上作業保証設備、深海ステーション、大型浮遊式構造物
先進起動交通設備	世界をリードする近代軌道交通産業体系
省エネ・新エネルギー自動車	電気自動車、燃料電池自動車
電力設備	新エネルギー・再生可能エネルギー設備、スマートグリッド用送変電設備
農業用機械設備	大型高効率コンバインハーベスター、農業生産の情報化
新材料	ナノ材料、グラフェン、バイオマス材料などの戦略的な先端材料
バイオ医薬・高性能医療器械	医療ロボット、モバイル医療製品、バイオ３Ｄ印刷、人工多能性幹細胞

戦術的インテリジェンス

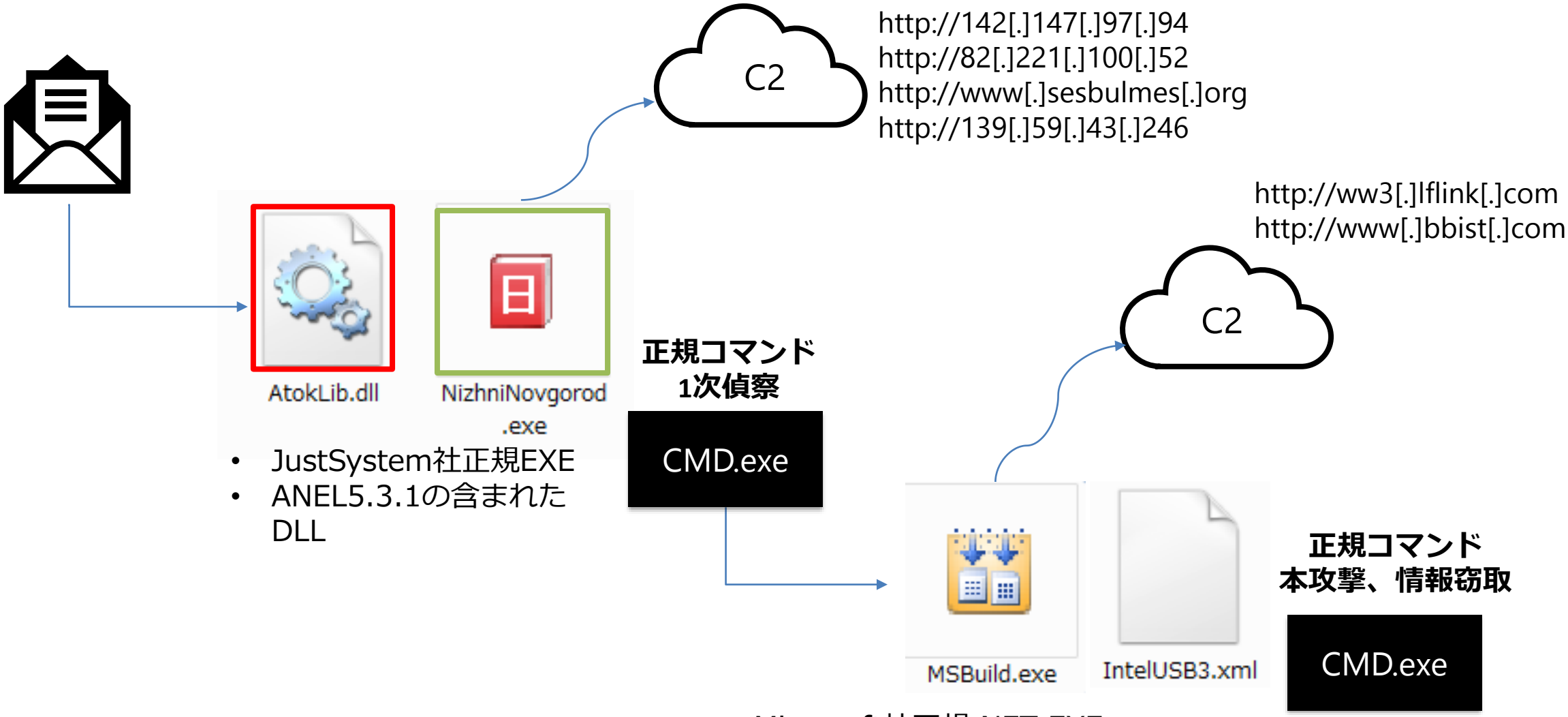
2018年に観測された標的型攻撃（マクニカ調べ）

APT10（ANEL マルウェア）





APT10（ANEL マルウェア）



APT10（一次偵察）

```
> 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
```

<- プロセスリスト
サービスのリスト
C:¥Users¥のファイルリスト

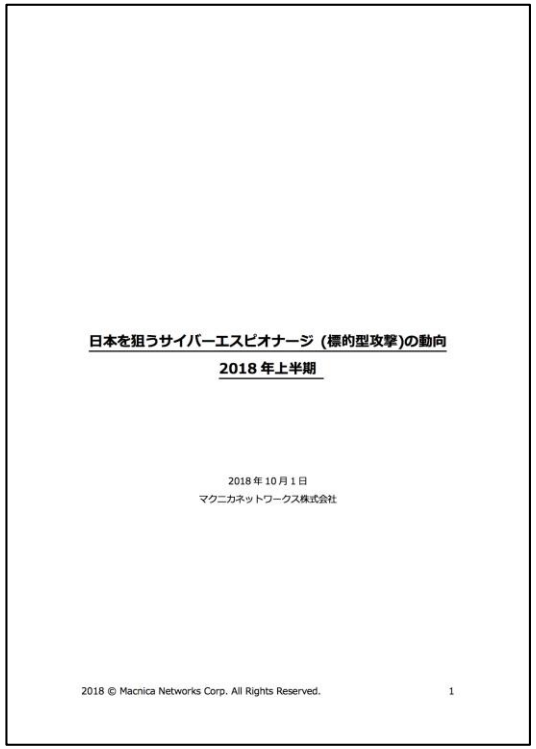
<- ANEL5.3.1の削除

APT10（情報窃取、OPSEC）

```
> taskkill /pid 2884 /f
> tasklist /v
> net start
> systeminfo
> reg query "HKC...Software\Microsoft\Windows\CurrentVersion\Run"
> %Temp%\ra...xe a -r -v500m %Temp%\%COMPUTERNAME%_.rar C:\Users\* -n*.doc* -n*.ppt* -n*.xls* -n*.jtd -n*.eml -n*.pst -hp"1enal5Sexy!" -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
```

一太郎系のファイルの窃取（= 日本を標的としている）

その他の情報については、こちらを



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

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。

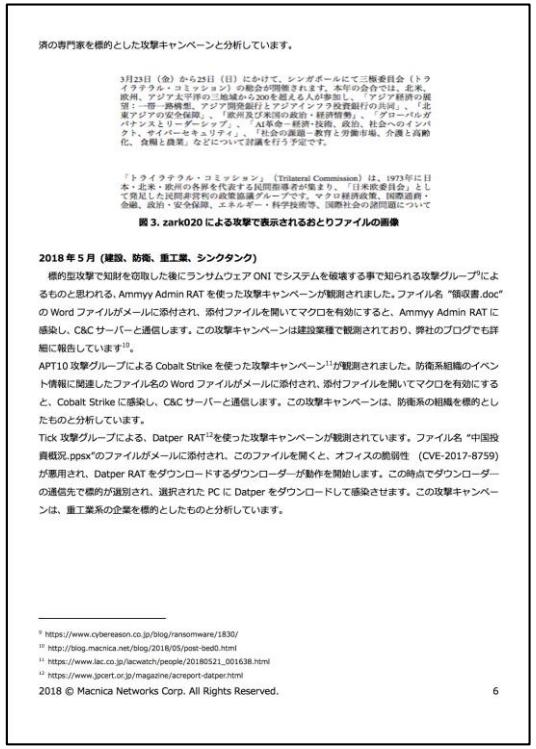
一般に公開されているブログ、リサーチペーパーでは、マルウェアのリバースエンジニアリング、暗号解読、攻撃者の特定といった視点が多くあり、検体解析やリサーチを行う分析者には大いに助けになります。一方、組織で対策を検討して、日々検出されたアラートに対応している情報セキュリティ担当者には敷居の高い情報かもしれません。本書では、組織の情報システムでセキュリティに携わっている方々へ効果的な注意喚起が図れるよう、観測された攻撃グループとその攻撃の TTPs。標的業種を表にし、脅威の検出に関しての考察を記載しています。対策手法のテクノロジーの進化に伴った際限のない投資から解き放たれ、自社が関連する業界を狙った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



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」、「社会の断面－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提議グループです。マクロ経済政策、国際通貨・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ーが動作を開始します。この時点でダウンローダー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

投資概況資料：中国
2018年5月

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。

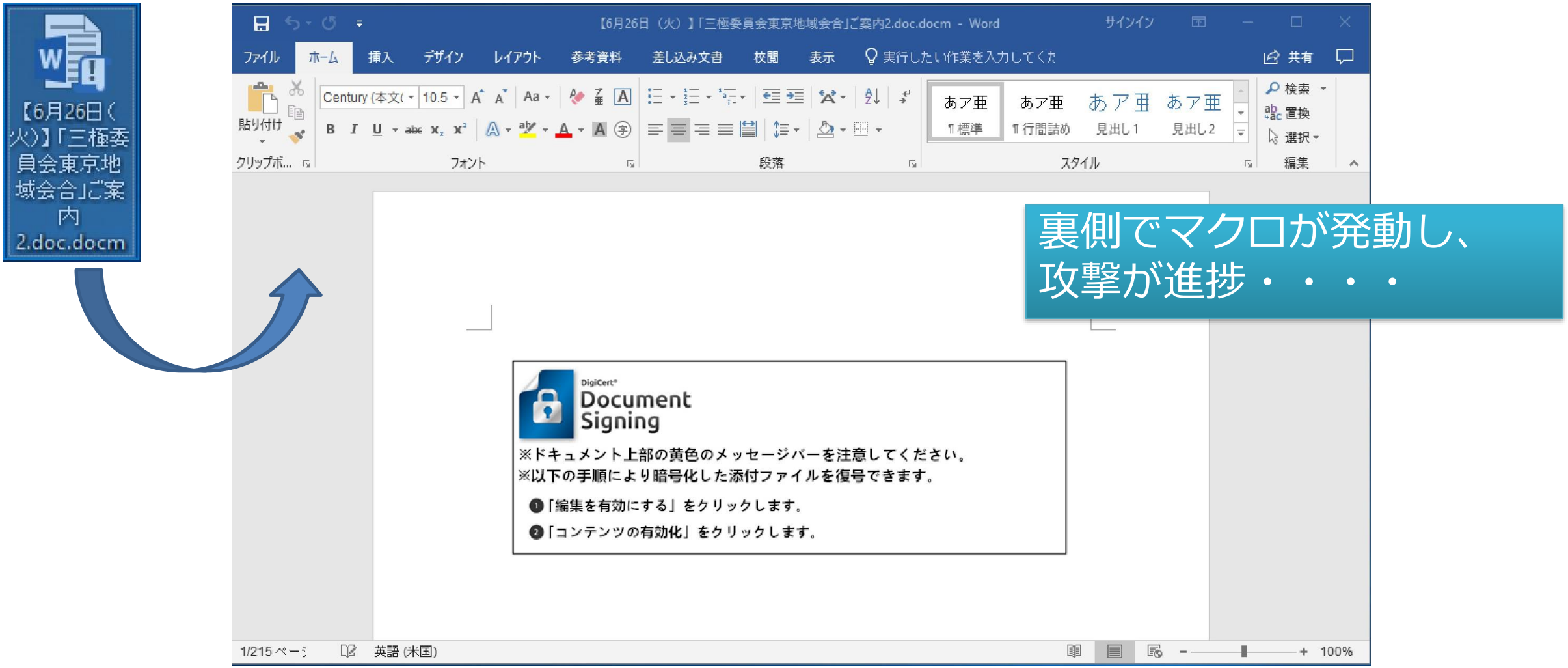
2018 年 7 月（メディア）

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]。

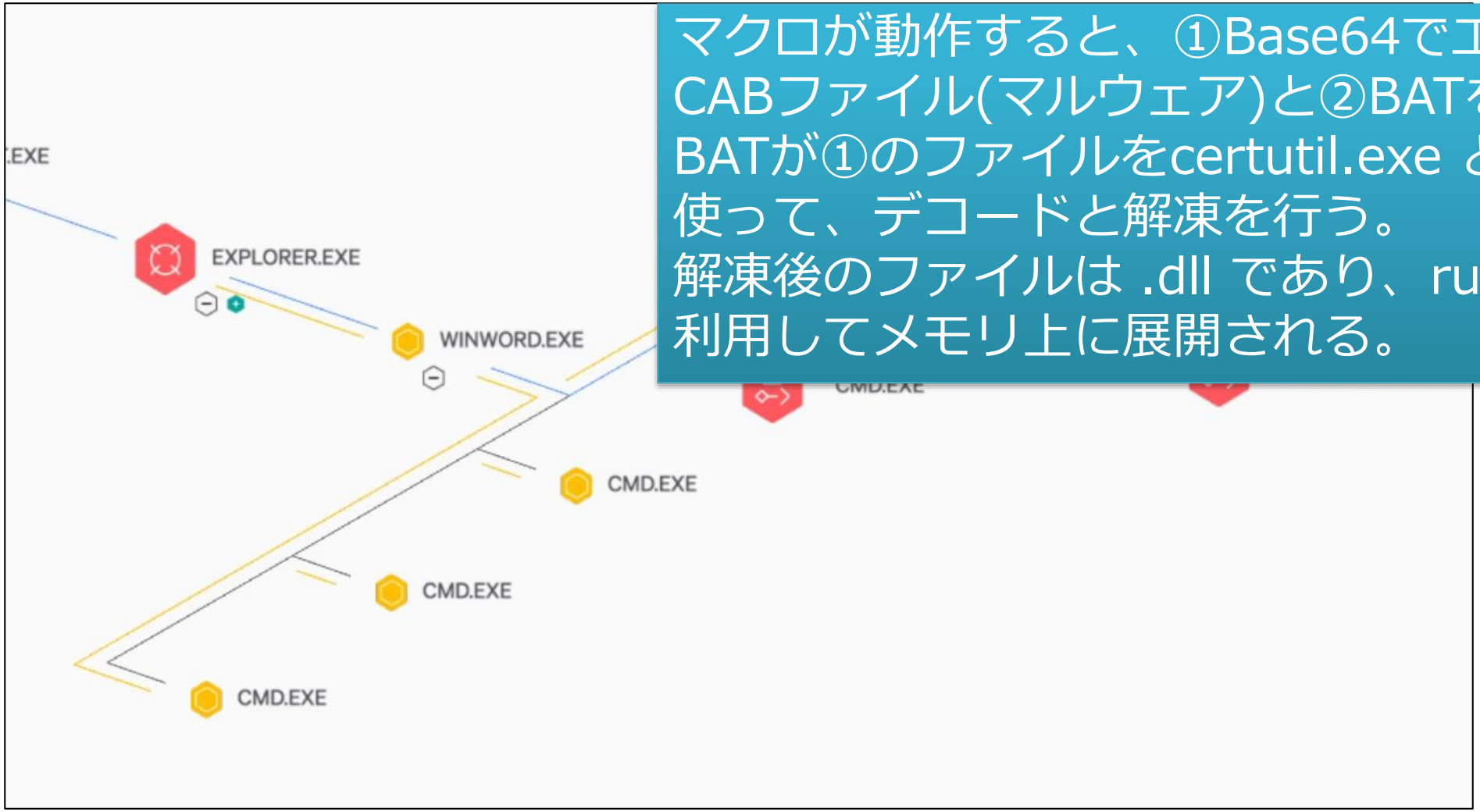
[13] https://blog.trendmicro.co.jp/archives/17280
[14] http://blog.macnica.net/blog/2018/08/post-5abc.html

Falcon vs APT

STONE PANDA/APT10

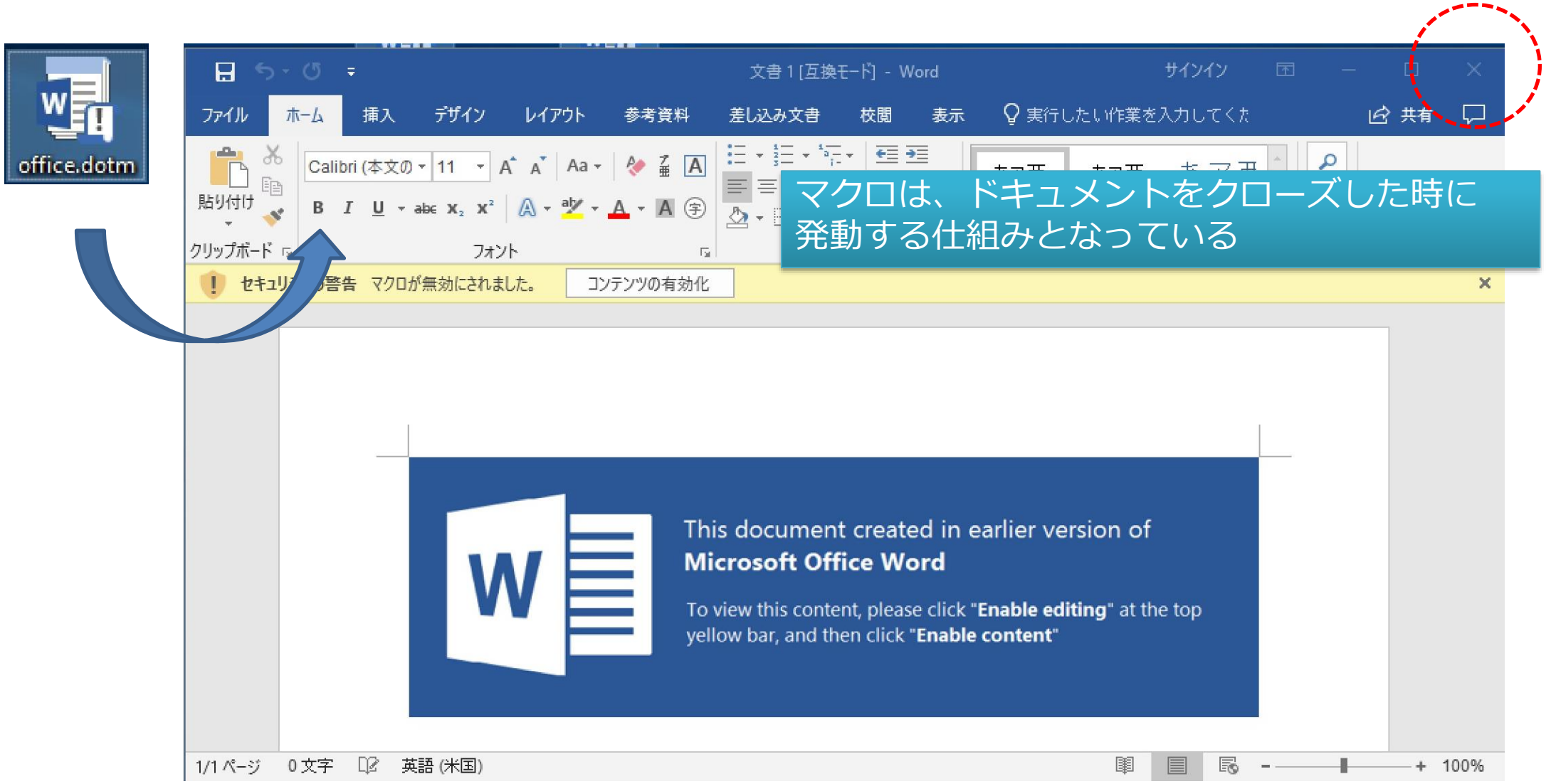


STONE PANDA/APT10

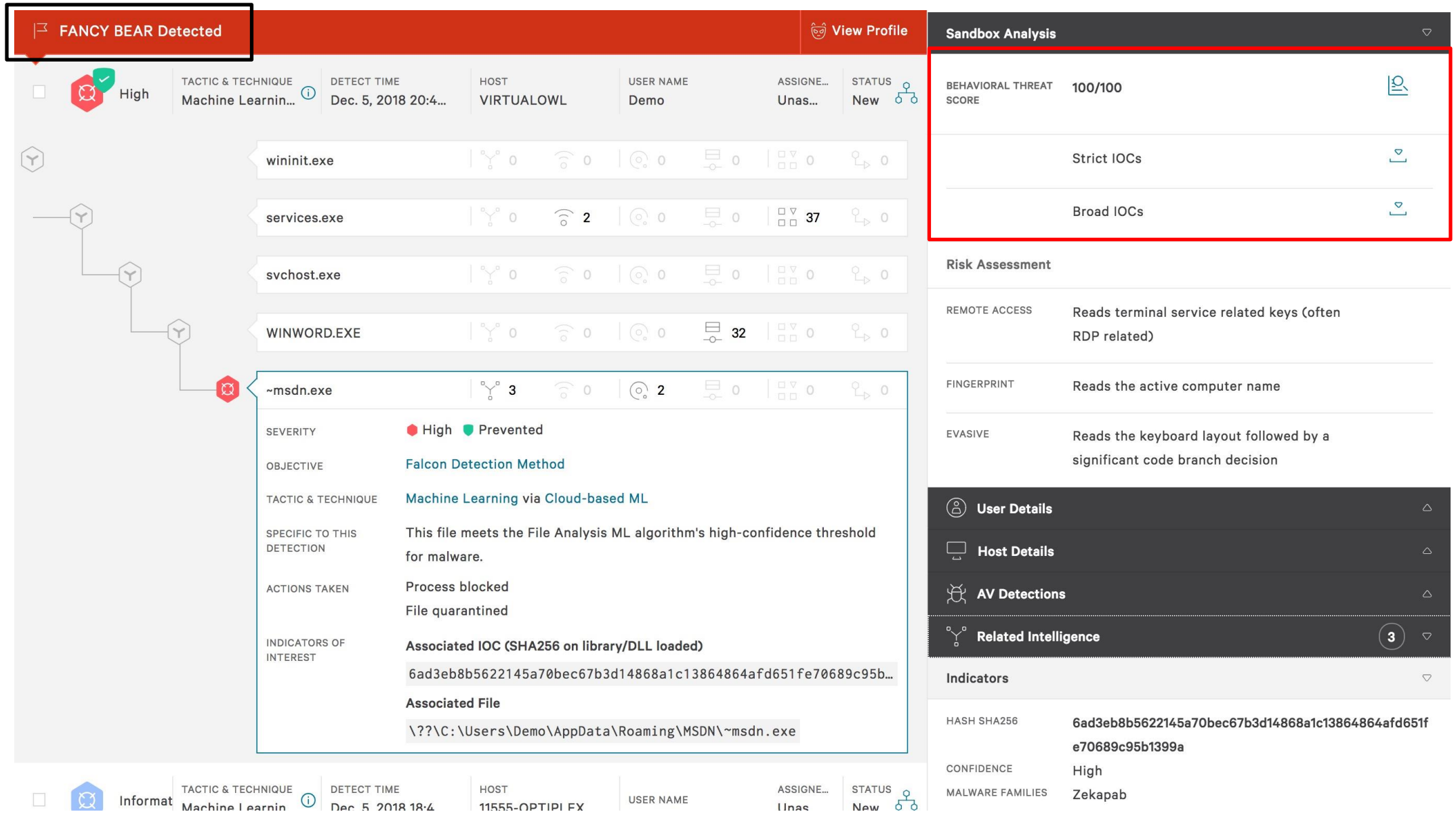


マクロが動作すると、①Base64でエンコードされたCABファイル(マルウェア)と②BATをドロップ。
BATが①のファイルをcertutil.exe とexpand.exeを使って、デコードと解凍を行う。
解凍後のファイルは .dll であり、rundll32.exe を利用してメモリ上に展開される。

FANCY BEAR/APT28



FANCY BEAR/APT28



FANCY BEAR/APT28

All reports | Sandbox Report - 6ad3eb8b5622145a70bec67b3d14868a1c13864864afd651fe70689c95b1399a | DOWNLOAD IOCS | PRINT

6ad3eb8b5622145a70bec67b3d14868a1c13864864afd651fe70689c95b1399a

SHA256
6ad3eb8b5622145a70bec67b3d14868a1c13864864afd651fe70689c95b1399a

THREAT LEVEL
▲ Malicious

THREAT SCORE
100/100

ANALYSIS
Detonated Dec. 5, 2018 20:42:47
Sandbox OS: Windows 7 32, Professional, 6.1 (build 7601), Service Pack 1

TAGGED GROUP-4127 PAWNSTORM STRONTIUM SWALLOWTAIL TG-4127 EVASIVE FANCYBEAR TSARTEAM TSAR TEAM GROUP74 SOFACY SEDNIT IRONTWILIGHT TAG_0700 TARGETED FANCY BEAR APT28 ZEKAPAB

REPORT SUMMARY | NETWORK ACTIVITY | ADVANCED ANALYSIS

Associated actor | Risk assessment | MalQuery | MITRE ATT&CK™ Tactics and Techniques | Behavioral threat indicators | File information | Screenshots

Associated actor

Show profile

ACTOR
FANCY BEAR

ORIGIN
Russian Federation

LAST KNOWN ACTIVITY
November 2018

COMMUNITY IDENTIFIERS
APT28, Sofacy, Tsar Team, Sednit

RELATED INDICATORS
Search

TARGET INDUSTRIES
Aerospace & Defense, Energy, Government, Hospitality, Media & Publishing, NGO/International Organizations

TARGET NATIONS
Belarus, Belgium, Brazil, Bulgaria, Canada, China, France, Georgia, Germany, Hungary, Iran, Japan, Latvia, Malaysia, Montenegro, Netherlands, Poland, Romania, Slovakia, South Korea, Spain, Sweden, Switzerland, United Kingdom, United States

FALCON INTELLIGENCE
FANCY BEAR is an adversary with a suspected nexus to the Russian Federation that carries out targeted intrusion primarily against North Atlantic Treaty Organization (NATO) member states and targets related to sensitive Russian issues such as international politics and sports. FANCY BEAR operations have been identified since at least 2012 and include spear phishing campaigns that deliver malicious ...

ご清聴ありがとうございました
Thank you for your attention