



Falcon Day vol.4

脅威インテリジェンスとFalconの防衛

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

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

■ 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

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

攻撃手法

■ 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**

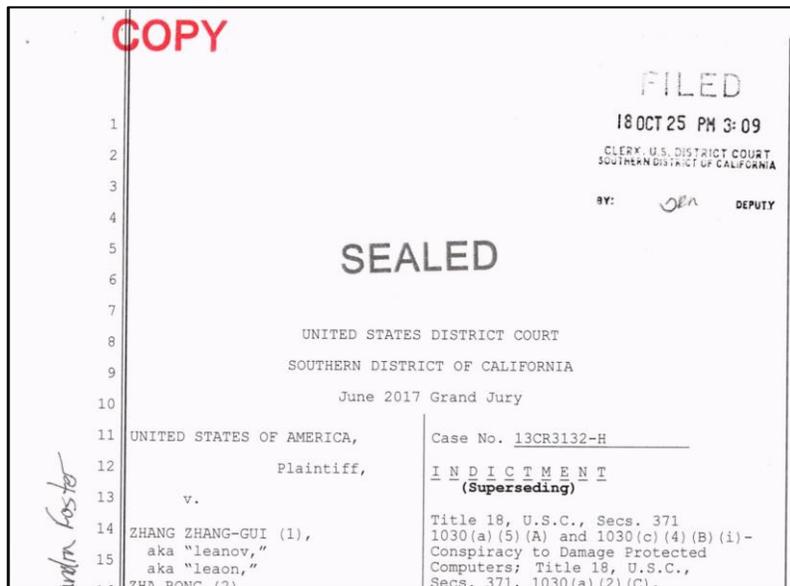
■ 米国司法省によって中国人に対する2つの起訴が発生

- 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>

- “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)



<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>

- “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)

WICKED PANDA 



LAST ACTIVE
October 2018

TARGET NATIONS
5 Germany, Japan, South Korea, Taiwan, United Sta...

TARGET INDUSTRIES
7 Chemicals, Engineering, Hospitality, Manufacturi...

YU PINGAN a.k.a. "GoldSun"



マルウェア
の譲渡



SAMURAI PANDA 



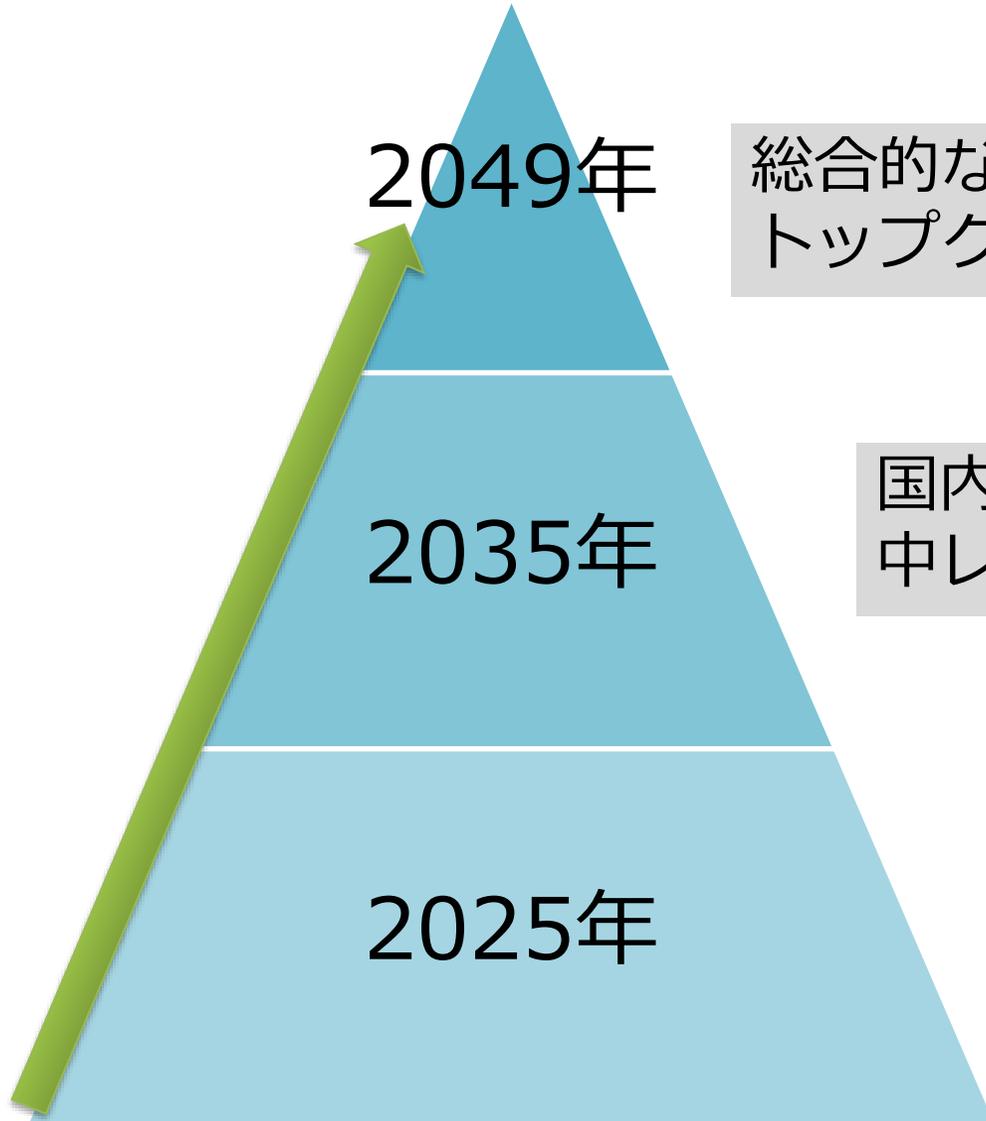
LAST ACTIVE
July 2015

TARGET NATIONS
1 Japan

TARGET INDUSTRIES
3 Aerospace & Defense, Financials, Government

<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>



2049年

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

2035年

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

2025年

製造強国に仲間入りすること

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

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)

	18/04	18/05	18/06	18/07	18/08	18/09
Tick (XXMM / Datper)	Group Targeted	重工業			化学、ハイテク関連製造	
Winnti	化学・燃料、ハイテク関連製造					
Ammy Admin		建設関連				
APT10 (RedLeaves-zark20rk)	シンクタンク					
APT10 (ANEL)		シンクタンク	メディア	メディア		
APT10 (Cobalt Strike / Quasar RAT)		防衛関連			メディア	
BlackTech (PLEAD)	政治関連					海洋関連
Taidoor (Taidoor / Taleret / Yalink)	ハイテク関連製造、通信キャリア					
DarkHotel					メディア	

吹浦忠正

2018年7月26日 12:22:41 JST

宛先: [redacted]

返信先: 吹浦忠正

Re: グatemala講演会

各位

添付をご覧ください。パスワードは c9690vvjo です。

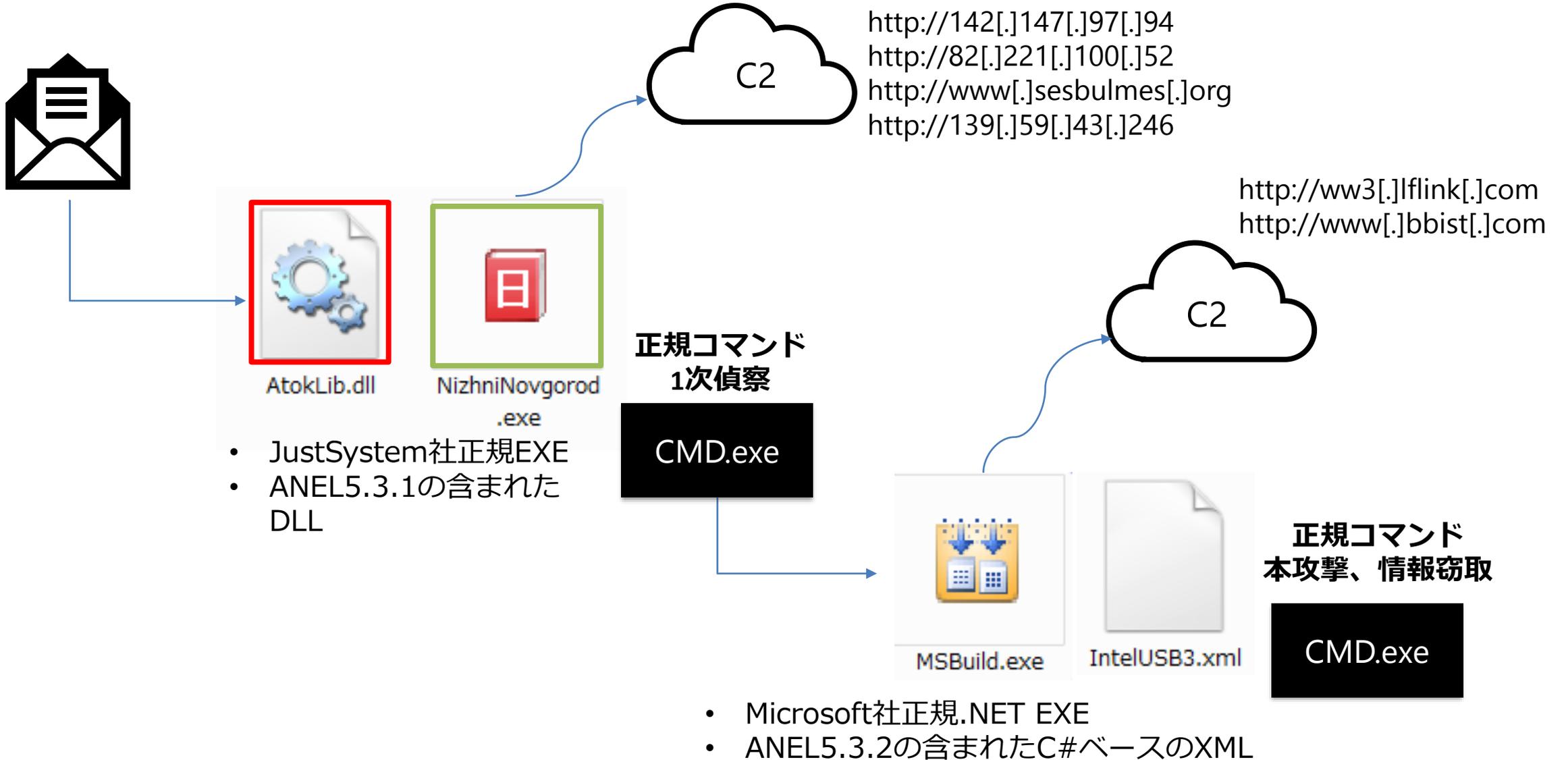
吹浦忠正



グatemala大使講演会案内状.doc

セキュリティの警告 マクロが無効にされました。 コンテンツの有効化

古谷朋彦 駐グatemala日本大使講演会「中米グatemalaの現状、課題と展望」【日時】 2018年 8月 9日 (木) 15:00~16:30 【会場】 日比谷国際ビル B1 会議室 (日比谷国際クリニック検診センター右隣) 東京都千代田区内幸町 2-2-3 Tel: 03-3591-3831 【主催】 一般社団法人ラテンアメリカ協会【講演題】「グatemalaの現状、課題と展望」【講師】 古谷 朋彦 駐グatemala特命全権大使【参加費】 会員 2,000 円、非会員 3,000 円 / 大学院・大学生 無料【備考】①申込み受付: 先着順 50名までです。お早めに以下からお申込み下さい。②申込締め切り: 平成 2018年 8月 6日 (月) 以下 WEB サイトからお申し込みください。URL: <https://latin-america.jp/seminar-entry>【詳細チラシ】(PDF) こちらをクリック【ラテンアメリカ協会】〒100-0011 東京都千代田区内幸町 2-2-3 日比谷国際ビル 120ATel: 03-3591-3831 Fax: 03-6205-4262 E-mail: info@latin-america.jp



```
> dir
> powershell "Get-WmiObject -Namespace 'root\SecurityCenter2' -Query 'SELECT * FROM AntiVirusProduct' | select-object
displayname,pathToSignedReportingExe,timestamp| fl"
> C:\Users\[REDACTED]\Desktop
> tasklist /v          <- プロセスリスト
> net start           サービスのリスト
> dir C:\Users\        C:¥Users¥のファイルリスト
> wmic LOGICALDISK get name,Description,filesystem,size,freespace
> more
> del c:\programdata\* /f /q <- ANEL5.3.1の削除
> 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
```

```
> taskkill /pid 2884 /f
> tasklist /v
> net start
> systeminfo                一太郎系のファイルの窃取 (= 日本を標的としている)
> reg query "HKC...oftware\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"1enal5Sexy!" -oc -ed -agyyymmdd
> 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
```

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

レポート公開中

<https://www.macnica.net/mpressioncss/report.html/>

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発達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数回の高情報な情報もありません。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、発達の検出に関する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放され、自社に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、製造データを盗む狙い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。

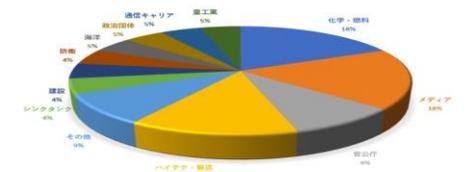


図1. 標的組織のバイチャート

¹⁾ https://media.socmagazine.com/documents/292/cloud-hopper-report-final-upda_72977.pdf
2018 © Macnica Networks Corp. All Rights Reserved.

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機委員会(トライラテラル・コミッション)の機会が開催されました。本年の機会では、米、英、露、印、アジア太平洋の三国から300名を超える人の参加し、アジア経済の展望―一帯一路戦略、アジア開発銀行とアジアインフラ投資銀行の共同、北米アジアの貿易関係、「東アジア米国の政治・経済情勢」、「グローバル・パナシスリーダーシップ」、「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、金融と高齢化、気候と農業、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・米・欧州の各首脳を代表する民間リーダーが集まり、「日米欧委員会」として設立した民間非営利の国際組織グループです。マクニカ経済政策、国際貿易・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. zarf020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によるものと推測される、Ammy 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「簡収書.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、Ammy Admin RAT に感染し、C&C サーバと通信します。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²⁾。

APT10 攻撃グループによる Cobalt Strike を使った攻撃キャンペーン³⁾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 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 RAT⁴⁾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、オフィス系の脆弱性(CVE-2017-8759)が適用され、Datper RAT をダウンロードするダウンロードが動作を開始します。この時点でダウンロードの通信先で標的が識別され、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。

²⁾ <https://www.cyberesson.co.jp/blog/ransomware/1830/>
³⁾ <https://blog.macnica.net/blog/2018/05/post-bed0.html>
⁴⁾ https://www.jac.co.jp/news/press/20180521_001638.html
⁵⁾ <https://www.geart.co.jp/magazine/report-datper.html>
2018 © Macnica Networks Corp. All Rights Reserved.

投資概況資料：中国



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 RAT⁵⁾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、オフィス系の脆弱性(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、これを開くと、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。

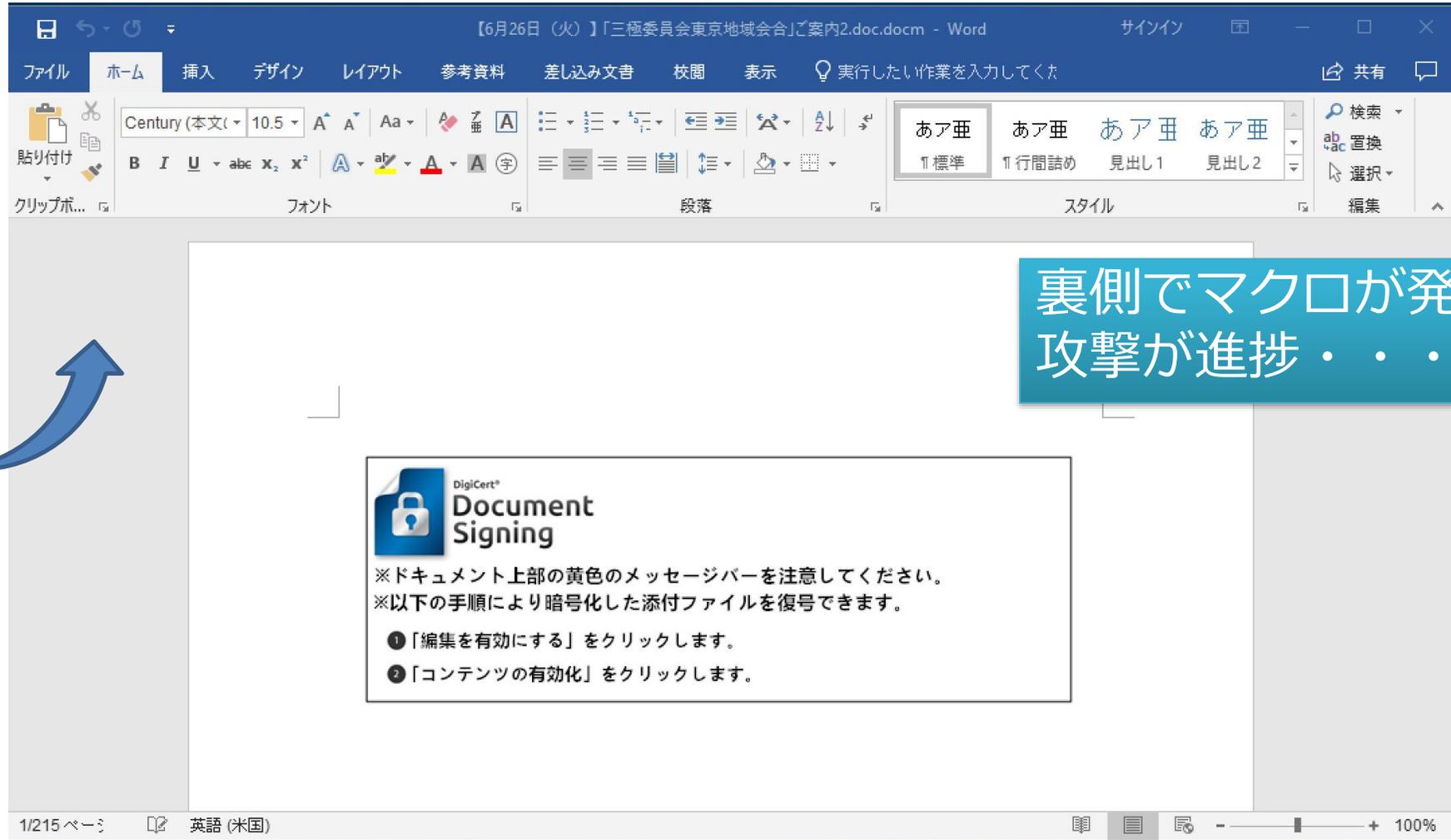
2018年7月(メディア)

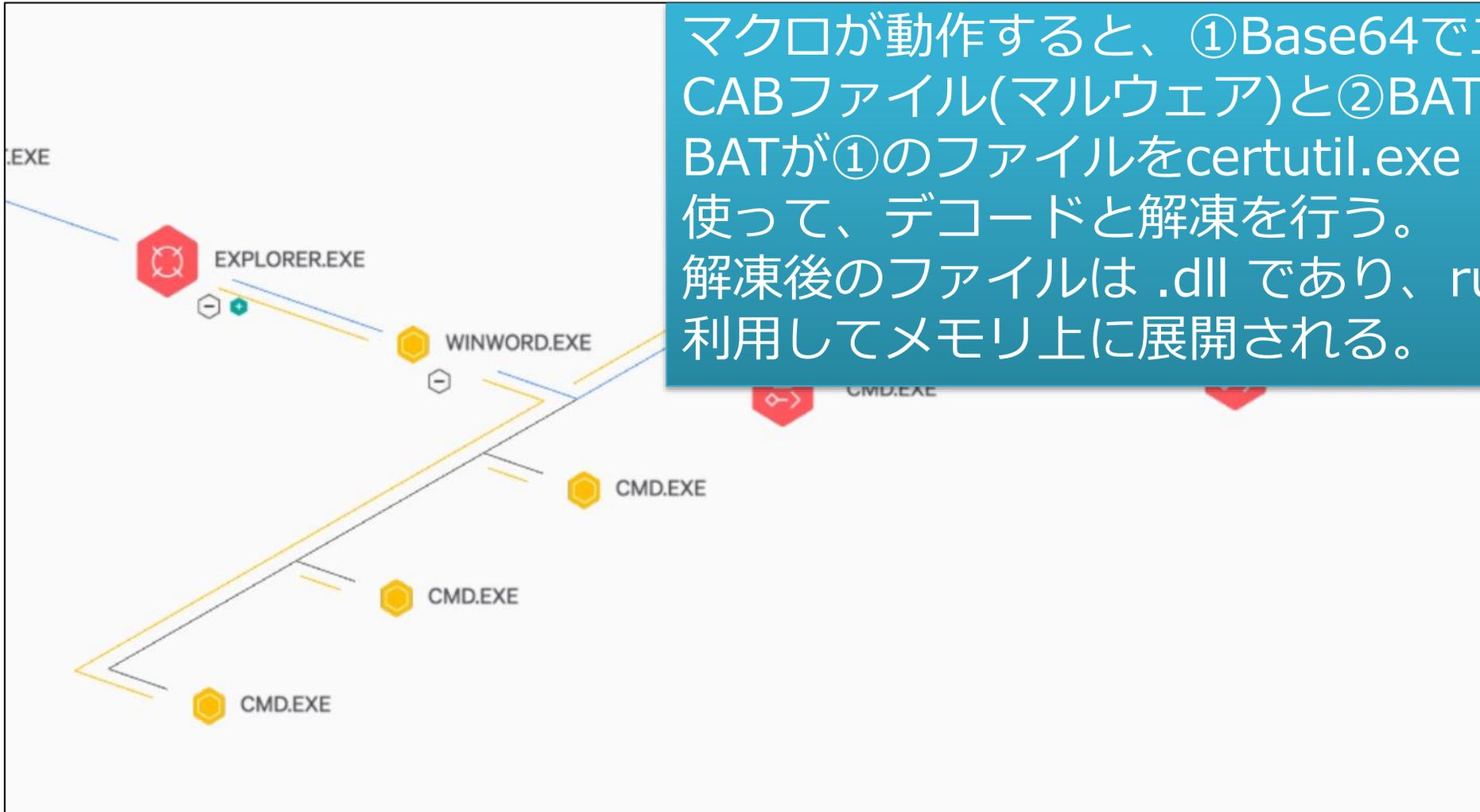
APT10 攻撃グループによる、Cobalt Strike を使った攻撃キャンペーンが引き続き観測されています。標的となった業種はメディア業種と分析しており、攻撃手法の詳細や弊社ブログに記載しています⁶⁾。

⁵⁾ <https://blog.trendmicro.co.jp/archives/17280>
⁶⁾ <http://blog.macnica.net/blog/2018/06/post-5abc.html>
2018 © Macnica Networks Corp. All Rights Reserved.

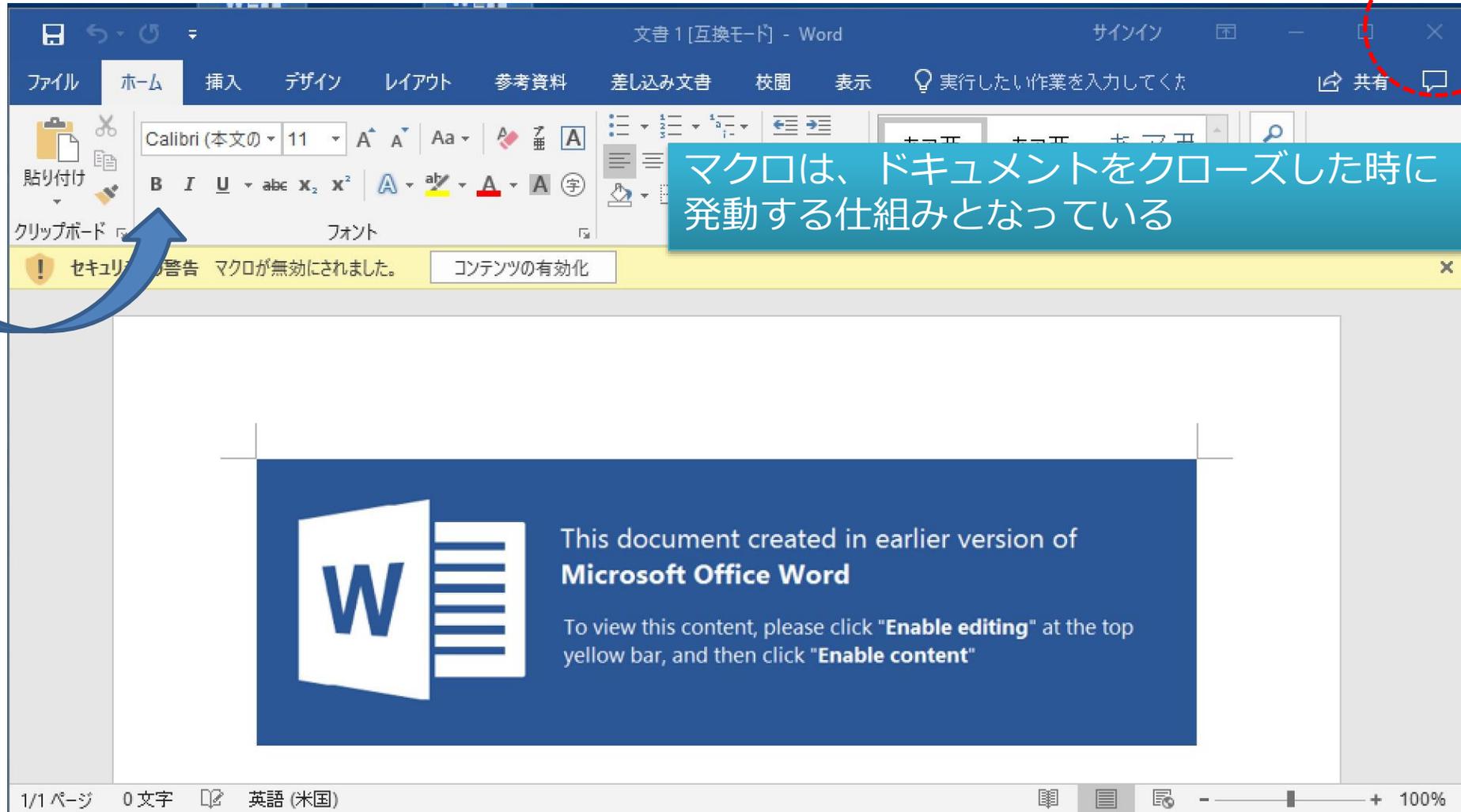
Falcon vs APT

【6月26日（火）】「三極委員会東京地域会合」ご案内 2.doc.docm





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。



文書 1 [互換モード] - Word

サインイン

共有

ファイル ホーム 挿入 デザイン レイアウト 参考資料 差し込み文書 校閲 表示 実行したい作業を入力してくた

Calibri (本文の) 11 A⁺ A⁻ Aa 文字書式

貼り付け

クリップボード

セキュリティ警告 マクロが無効にされました。 コンテンツの有効化

マクロは、ドキュメントをクローズした時に発動する仕組みとなっている

This document created in earlier version of Microsoft Office Word

To view this content, please click "Enable editing" at the top yellow bar, and then click "Enable content"

1/1 ページ 0 文字 英語 (米国) 100%

FANCY BEAR Detected
View Profile

Status	Severity	TACTIC & TECHNIQUE	DETECT TIME	HOST	USER NAME	ASSIGNE...	STATUS
<input type="checkbox"/>	High	Machine Learnin...	Dec. 5, 2018 20:4...	VIRTUALOWL	Demo	Unas...	New

winit.exe	0	0	0	0	0	0	0
services.exe	0	2	0	0	0	37	0
svchost.exe	0	0	0	0	0	0	0
WINWORD.EXE	0	0	0	0	32	0	0
~msdn.exe	3	0	2	0	0	0	0

SEVERITY ● High ● Prevented

OBJECTIVE [Falcon Detection Method](#)

TACTIC & TECHNIQUE [Machine Learning via Cloud-based ML](#)

SPECIFIC TO THIS DETECTION This file meets the File Analysis ML algorithm's high-confidence threshold for malware.

ACTIONS TAKEN
Process blocked
File quarantined

INDICATORS OF INTEREST
Associated IOC (SHA256 on library/DLL loaded)
6ad3eb8b5622145a70bec67b3d14868a1c13864864afd651fe70689c95b...

Associated File
\\?.\C:\Users\Demo\AppData\Roaming\MSDN\~msdn.exe

Status	TACTIC & TECHNIQUE	DETECT TIME	HOST	USER NAME	ASSIGNE...	STATUS
<input type="checkbox"/>	Informat Machine Learnin	Dec. 5, 2018 18:4	11555-OPTIPI FX		Unas	New

Sandbox Analysis

BEHAVIORAL THREAT SCORE	100/100	🔍
Strict IOCs		📄
Broad IOCs		📄

Risk Assessment

REMOTE ACCESS	Reads terminal service related keys (often RDP related)
FINGERPRINT	Reads the active computer name
EVASIVE	Reads the keyboard layout followed by a significant code branch decision

User Details

Host Details

AV Detections

Related Intelligence 3

Indicators	
HASH SHA256	6ad3eb8b5622145a70bec67b3d14868a1c13864864afd651fe70689c95b1399a
CONFIDENCE	High
MALWARE FAMILIES	Zekapab

← All reports

Sandbox Report - 6ad3eb8b5622145a70bec67b3d14868a1c13864864afd651fe70689c95b1399a

DOWNLOAD IOCS

PRINT

6ad3eb8b5622145a70bec67b3d14868a1c13864864afd651fe70689c95b1399a



SHA256

6ad3eb8b5622145a70bec67b3d14868a1c13864864afd651fe70689c95b1399a

THREAT LEVEL i

▲ Malicious

THREAT SCORE i

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

- 本資料に記載されている会社名、商品、サービス名等は各社の登録商標または商標です。なお、本資料中では、「™」、「®」は明記しておりません。
- 本資料は、出典元が記載されている資料、画像等を除き、弊社が著作権を有しています。
- 著作権法上認められた「私的利用のための複製」や「引用」などの場合を除き、本資料の全部または一部について、無断で複製・転用等することを禁じます。
- 本資料は作成日現在における情報を元に作成されておりますが、その正確性、完全性を保証するものではありません。